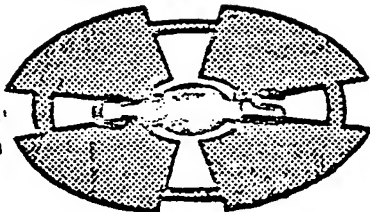


Community On-Line Intelligence System

Project Management Office

National Security Agency

Fort George G. Meade, Maryland, 20755



COINS LONG-RANGE PLAN

PART III

TECHNICAL SUPPORT PLAN (TSP)

FY80 - FY86

Prepared by
The MITRE Corporation
7 August 1980

ACKNOWLEDGEMENT

Many individuals made significant contributions to the COINS Network Technical Support Plan. Specifically; H.A. Kinslow of H. Kinslow Associates, Inc. contributed Section 2, Background, and James P. Anderson of James P. Anderson Company contributed Annex D, COINS Network Security. The author is indebted to the above named individuals who, together with [REDACTED] [REDACTED] and Richard W. Bates, consultant to Computer Sciences Corporation, spent many hours reviewing previous versions of this plan and made many valuable suggestions and provided much of the information needed to bring it to its present form.

Any errors of omission or commission are the sole responsibility of the author.

TABLE OF CONTENTS

	<u>Page</u>
1.0 INTRODUCTION	1
1.1 Purpose	1
1.2 Organization	2
2.0 BACKGROUND	3
2.1 Current Status	6
2.2 Future Development	7
2.3 Background Summary	12
3.0 FACTORS INFLUENCING THE PLANS	13
3.1 Facts	13
3.2 Assumptions	14
4.0 SUMMARY OF TECHNICAL SUPPORT PLANS	15
4.1 COINS Network Management	15
4.2 COINS Network Resources	16
4.3 COINS Network Development	19
4.4 COINS Network Security	20
4.5 Resource Summary	22
GLOSSARY	24

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	COINS II Ring Architecture Concept	5
2	COINS PMO Controlled Resources	17

1.0 INTRODUCTION

This is Part III of the three-part COINS Long-Range Plan. Part I presented the COINS operations concepts as they are today, and as they are projected to be in 1985 and in 1990. Part II presented the COINS architecture in a similar fashion—as it is today, and projected to 1985 and 1990. Parts I and II of the plan were developed to provide the reader with an understanding of how the COINS PMO perceived the evolution of COINS during the 1980's, and to provide a basis and direction for the COINS PMO planning, programming and budgeting activities. Part III, Technical Support Plan, of the COINS Long-Range Plan presents the program plans, resources, and schedules to develop and maintain COINS for the current fiscal year and five years beyond.

1.1 Purpose

The purposes of Part III of the COINS Long-Range Plan are:

- a. To support the COINS PMO planning, programming, and budgeting activities and COINS-related planning, programming, and budgeting activities of the other organizations participating in COINS.
- b. To describe, for the COINS community and other interested organizations, the development and acquisition of new and improved COINS capabilities.
- c. To provide the planned development, procurement, and implementation schedules for use by COINS participating organizations in scheduling their planned development, procurement, and implementation actions that may be impacted by or impact on COINS.
- d. To provide resource estimates to development and maintain COINS.

1.2 Organization

Section 2 of Part III provides a description of COINS. It contains much of the introductory material of Parts I and II of the Long-Range Plan and is included here to provide the readers who had not read either Part I or Part II of the COINS Long-Range Plan with a basic understanding of COINS.

Section 3 presents major factors that were considered in developing the TSP. Section 4 is a summary of the planning activities and resources included in Annexes A, B, C, and D. Finally, the Annexes provide the Technical Support Plans.

Annex A - COINS Network and Project Management

Annex B - COINS Network Resources

Annex C - COINS Network Development

Annex D - COINS Network Security

2.0 BACKGROUND

This section presents the history of COINS development since 1965, and projects its further development through the end of this decade.

The objective of COINS is to serve the analysts of the intelligence community in retrieval and analysis of intelligence data. It is operational as a communications medium between several of the data processing centers of the community and is in increasing use for data retrieval from these centers.

However, its utility as a service to intelligence analysts is limited in many ways. Much information which should be available via COINS is not available. Procedures for access are complex and there are many different procedures to be learned. Data processing services are very sparse.

The COINS plan for development during the 1980's is to:

- Widen the base of the network by increasing its data resources
- Simplify, for the analyst, the procedures of retrieving data
- Provide assistance in processing of data once it is retrieved
- Provide network-wide user services such as electronic mail and teleconferencing

This initial section presents the history of COINS, and describes the environment which bounds its development. The network originated in 1965 as an experimental, store-and-forward network, and became

operational in 1973. In 1974 it began a process to upgrade from a store-and-forward to a packet-switched technology. The packet-switched network was declared operational as COINS II in 1977. Since then it has continued to evolve in scope and in service.

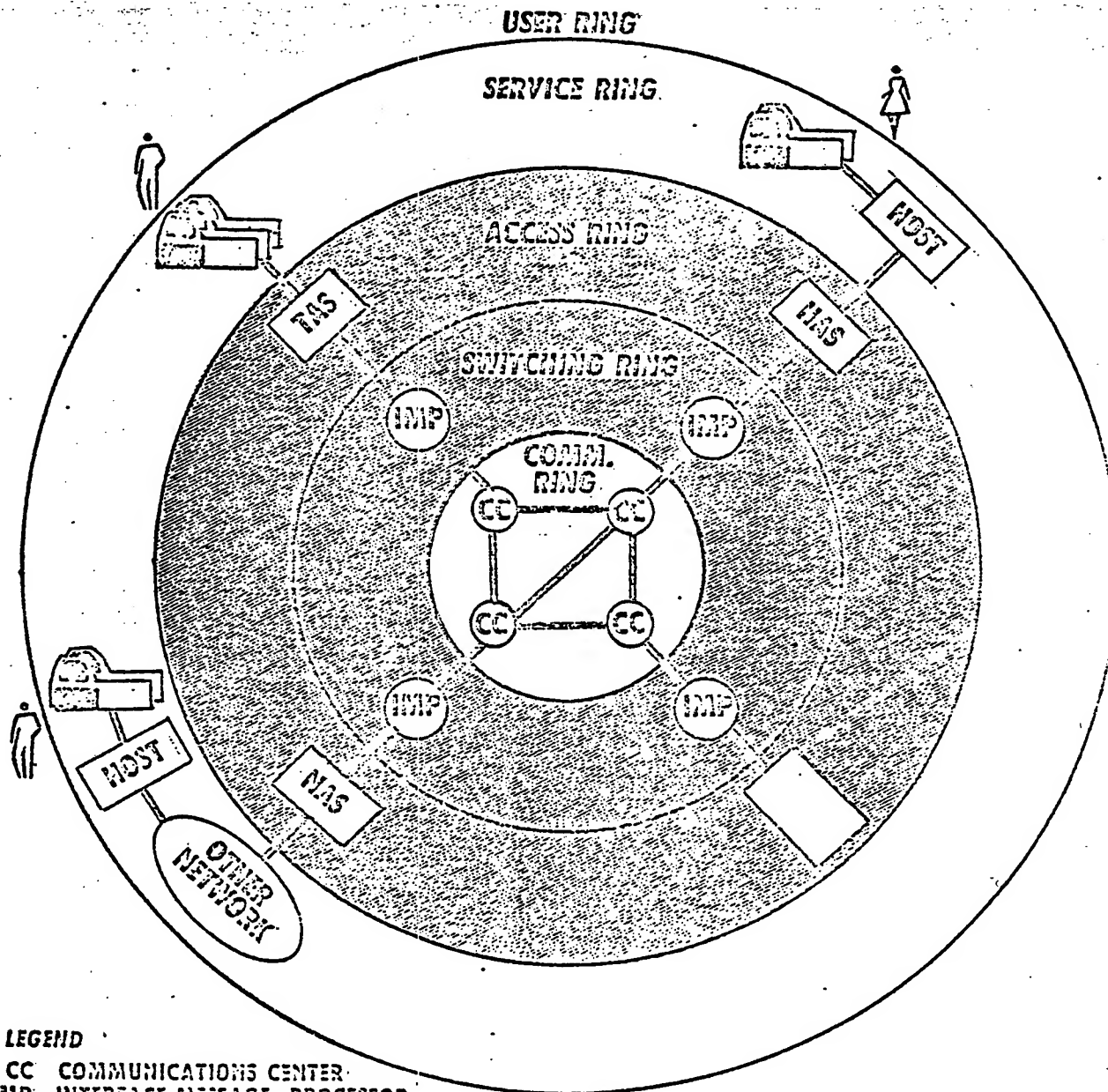
The COINS environment is the community of analysts, the data base systems extant and projected, the methods and procedures which COINS must adapt to, and other DoD networks with which COINS will interact.

Figure 1 presents a general description of COINS as a set of functional rings:

- The Communications Ring is the basic data transmission facility.
- The Switching Ring contains the COINS packet switching nodes.
- The Access Ring contains the devices which attach terminals and data processing systems to COINS, and through which COINS connects to other networks.
- The Service Ring contains the COINS host systems, processing systems and services, and terminals including those in other networks.

Each of the preceding rings contains a set of communications or service functions, supported by an inner ring, and supporting an outer ring.

- The User Ring. Outside the service ring are the users of COINS--the reason the four inner rings exist.



LEGEND



CC COMMUNICATIONS CENTER
 IMP INTERFACE MESSAGE PROCESSOR
 TAS TERMINAL ACCESS SYSTEM
 HAS HOST ACCESS SYSTEM
 NAS NETWORK ACCESS SYSTEM
 COINS PMO ZONE OF CONTROL
 TERMINALS

FIGURE 1

COINS II

RING ARCHITECTURE CONCEPT

2.1 Current Status

Six computer systems are directly connected to the COINS II network--NSA RYE/TIPS, NPIC NDS, NSA SOLIS, the COINS PMO TAS, the COINS PMO Network Service Host, and the PACOM TAS (via the ARPANET Gateway). Only the TAS-based systems can access SOLIS.

NSA RYE/TIPS, DIA DIAOLS, the processors at ADCOM and PACAF, and, in the future, the Network Service Host, function as both server and user hosts, i.e., they provide information retrieval services for COINS users, as well as link their own user terminals to COINS. SOLIS acts only as a server-host. The COINS PMO TAS, the PACOM TAS, the PACOM IDHSC SWITCH, and the processors at SAC and IPAC support user terminal connections to COINS but provide no services to COINS users.

NSA RYE/TIPS user terminals cannot interact with remote interactive hosts. The COINS II accessible files of RYE/TIPS will be installed on the interactive PROJECTOR when they are to be moved to WINDMILL system; a Burroughs 7700 dual processor currently housing SOLIS.

The NPIC New Data System (NDS) is connected to COINS by an adaptation of the TAS, called the Network Access System (NAS). Via the NAS, local NPIC terminals are currently able to work in batch mode with other COINS II hosts as if they were TAS terminals. During the first year of NDS operation with COINS, COINS II users will access NDS in batch mode only, although interactive capability exists. By the end of calendar year 1980 NPIC will offer both batch and interactive services to COINS.

Network services between COINS and IDHSC continue to be limited to batch transactions since the protocols and gateway software to handle interactive connections between COINS II and IDHSC have not been defined.

2.2 Future Development

To date, development of COINS has concentrated on communications systems in order to provide an instrument for remote access from a single point of entry (terminal) to intelligence data at several centers of storage (data base systems). The access capability that now exists is constrained in some ways:

- Some of the community data bases are not accessible from COINS terminals. Their host computers are not attached to COINS, or to a network which can be reached via COINS, or their security and need-to-know controls cannot be handled by COINS.
- Access from some points is limited by the interface between user and COINS. For example, an analyst at an IDHSC terminal cannot access the SOLIS system. The necessary interactive protocols cannot be propagated through the gateway between IDHSC and COINS, and in many instances the analyst does not have the proper remote terminal.

Removal of these constraints is a matter of resources and time. Most of them will disappear as older host systems are replaced, or as the present DoD network environment evolves.

Beyond mere access to data, the COINS users need help in other areas:

- Learning procedures for data retrieval. The COINS user is currently required to know where data is, and for each source of data, the language which must be used to extract from it.

- Manipulation and formatting of data once extracted from the file is done by the host computer on which the file is stored. Having retrieved data, the analyst must then resort to pencil and paper to reduce it to a form appropriate for the intended purpose.

Present COINS provides little help in solution of these problems.

It is projected that development of COINS during the 1980's will concentrate on the problem of reconciling data formats and access languages. Some aspects of this problem are:

- Multiple Retrieval Languages. In general, each data base is accessed by a language unique to that data base. The user may require information from several data bases, and is thus faced with the need to learn more than one language.
- Host System Autonomy. COINS hosts are designed and operated to serve local needs. COINS has low priority relative to these local needs, and must work out methods of adapting to them.
- Lack of Data Standards. There is no common methodology for data definition. Data is categorized, structured, and named in many different ways, depending upon who "owns" it. To perform a complete search, the user must know all of the terminologies by which data may be referenced.
- Community Turnover. The user population is dynamic. New users are constantly entering the community. There is a continuous and massive problem of training them in the nature of resources available, and the methods for their exploitation.
- Security. There is no system for support of multi-level security. Access via COINS is restricted to the SI/TK level. Most of the potential intelligence community users are thus excluded from COINS.
- Undefined Network Command Language. There is no agreed upon set of commands, or command "language", for initiating and controlling network functions.

These problems have been under attack for some time. By the mid-1980's useful techniques for their solution should be implementable.

The second problem, provision of data manipulation services for the user, requires a better understanding of the analysts job and what tools would be helpful in performing it. Studies are being made. By the latter half of the decade COINS should be in a position to support the user with hardware and software which assists in analysis of data once it has been retrieved.

Development of functions within COINS will be influenced by expected changes in the COINS environment, among which may be cited:

- Cost of Components. Current equipment costs indicate that centralized processing for many functions is economical. However, if these costs continue to fall, it may become efficient to distribute function execution throughout the network.
- Advances in Security Methodology. COINS has been requested by ASD(C³I) to cooperate with DCA in development of a community standard, Secure Network Front-End. Project BLACKER is under development. The Kernelized Secure Operating System (KSOS) is also under development. These efforts may have significant impact on the methodology of access to COINS.
- Projected Increase in Traffic. Present Access Systems have fairly low capacity with respect to number of physical attachments which can be supported ("ports") and throughput capacity. The projected traffic far exceeds these limitations. Increase of Access System capacity to meet traffic demand may force complete redesign of Access System structure and function as well as influence the future designs of the host systems themselves.

- Network Access via Terminals. Most of the present COINS terminals are attached to hosts, and access the network through hosts. During the 1980's the trend will be to terminals which access hosts via a network. There will be a requirement for many Terminal Access Systems of very high capacity.
- Terminal Evolution. Many of the community systems presently support only line-oriented, hardcopy terminals. Newer systems employ CRT terminals, and increasingly, "intelligent" terminals.

This trend to increasing terminal functionality will obviously impact the methodology of network access.

The COINS environment includes other networks to which COINS will be connected. COINS itself is designed and operated to support U.S. intelligence agencies in the Washington, D.C. area. It either is or will be connected via "gateways" to a number of other networks; i.e.:

- ARPANET
- PLATFORM
- IDHSC
- AUTODIN II
- IAIPS

Development of these projected internetwork connections will be governed by changes in the Defense Department network structure:

- AUTODIN II will become operational as the DoD long-haul communications facility.
- The present ARPANET will be significantly reduced in size and retained as a research facility. Many of its present hosts will become hosts of AUTODIN II.

- The DODIIS hosts within the Washington, D.C. area will become hosts of COINS. DODIIS hosts outside of Washington will use AUTODIN II.

The impact of these changes on COINS development will be manifold;

- The COINS network will be expanded to support Washington, D.C. DODIIS hosts; specifically at DIA, NMIC, AFIS, and NAVINTCOM.
- New protocols such as File Transfer and Teleconferencing will be required.
- COINS may be required to provide DODIIS interconnectivity during the transition of IDHSC to AUTODIN II.
- The TETRAHEDRON communications system, which is the base of the COINS subnet, may require expansion to include Andrews AFB, Suitland, Maryland and Fort Detrick, Maryland, and to interface with AUTODIN II.
- Increased traffic against the more heavily used COINS hosts must be anticipated and provided for.
- COINS current use of ARPANET as a carrier to distant users will be replaced by AUTODIN II.
- COINS itself may be a carrier between facilities in adjacent networks.

The COINS network, and each of the five networks to which COINS will be connected, is providing operational service to a unique family of users. Each network, including COINS, has its own set of established protocols and services. These are not easily changed without considerable cost as well as user hardship. It is planned that connection of COINS to another network will not:

- Result in disruption of service to users in either network
- Result in major changes in protocols and services in either network

- Result in major software reprogramming action in either network

2.3 Background Summary

The COINS network is being developed as a tool for cooperative effort in intelligence data processing. It is a vehicle for supporting the individual efforts of some forty intelligence centers of the U.S. Government.

These centers are autonomous. Each of them has its own criteria for type of data, method of processing, equipment for processing, security control, and every other conceivable parameter. COINS, which is the technological medium for interaction between them, must resolve the differences.

It is obvious from preceding discussions that the data retrieval problems of the COINS environment are not all solved, and that the solution in many cases may be a long time coming. Much of the COINS effort in this decade will be expended on these problems.

Beyond the problems associated with data retrieval there are services which the network can provide. These must be defined to fit the needs of the analyst. The network can become a system for data processing which taps all resources of the community, at the analyst's convenience, and provides him with the tools for effective use of them.

3.0 FACTORS INFLUENCING THE PLANS

The following factors were considered in the development of the Technical Support Plans (Annexes A, B, C, and D).

3.1 Facts

COINS will continue to supply services beyond that of a conduit for data transmission to the COINS users. These include services that can be provided more efficiently by COINS than by the separate participating agencies; e.g., network access control, common query language (ADAPT), user support systems; and information storage and manipulation services for those users homed on a TAS who cannot or do not have these services provided by their parent organizations.

ASD(C³I), Executive Agent for the COINS program, has directed that:

- a. The TCP4/IP4 Host-to-Host protocol be implemented in COINS II, IDHSC II, AUTODIN II, and ARPANET as a first step towards achieving network interoperability. This will require modification to the IMP software and the Host Access System (HAS).
- b. AUTODIN II will be used as the long-haul communications facility by the mid-1980's, therefore, COINS II will be required to use AUTODIN II as the preferred conduit providing services outside the Washington, D.C. area vice ARPANET or IDHSC II.
- c. The COINS PMO will work with DCA in the development of a community standard front-end. The use of this front-end by COINS could have a significant impact on the COINS Access System.

The expanded COINS plus existing high turnover rate in COINS users, particularly in the military organizations, necessitates a continuing and increasing training work load.

3.2 Assumptions

The COINS will continue through the 1980's and be expanded to function as the local network for the Washington, D.C. area DODIIS host computers. DIA has informally designated COINS as the local Washington D.C. DODIIS network. It is assumed that this designation will be made formally, and the host computers involved will be identified along with procedures on how these hosts will be treated; i.e., like the existing COINS hosts or in some special ways. Until the designation is formalized and the hosts identified, etc., planning for the expansion cannot be completed.

Access to COINS should be expanded to the analysts with less than TS-SI/TK who need COINS accessible information. This requires improved security procedures to preclude unauthorized disclosure.

4.0 SUMMARY OF TECHNICAL SUPPORT PLANS

The objective of the COINS PMO is to provide, within available resources and other imposed constraints, the highest quality, secure services to the users of COINS and to the organizations who are the sponsors of COINS accessible resources--presently file sponsors.

4.1 COINS Network Management

To meet the objective, the COINS PMO must be aware of user and sponsor needs that are not being satisfied adequately in order that unsatisfied requirements can be addressed in the COINS program planning and budgeting. For this reason, resources have been programmed to acquire a network management system (hardware and software) that can monitor the status and performance of the hardware and software that comprise the COINS network and its accessible resources. Also, the management system will collect and analyze information relative to the usage of COINS and its accessible resources, and data relative to user acceptance and satisfaction of COINS.

The COINS Network Management System comprises:

- The Network Monitoring Subsystem (NMSS) - To collect and analyze status and performance data for operations and management
- The Network Usage Information Subsystem (NUISS) - To collect and analyze data relative to resource usage
- The User Reporting Subsystem (URSS) - To collect and analyze data relative to user satisfaction of COINS.

The Technical Support Plan for COINS Network Management is presented in Annex A.

By the end of FY82 the Network Monitoring Subsystem (NMSS) will be operational in the BBN C/70 Network Control Computer (NCC) and the BBN C/70 Network Management Computer (NMC). Also, the Network Usage Information Subsystem (NUISS) will be implemented on the Network Management Computer. The evaluation of the pilot User Reporting Subsystem (URSS) is scheduled to be completed by the end of FY82.

FY83 through FY86 will produce enhancements to NMSS and UNISS, and the operational URSS will be developed and implemented.

4.2 COINS Network Resources

The COINS-provided resources are the hardware and software included in the switching and access rings, and in COINS PMO-controlled service hosts computers in the service ring--see Figure 2.

The switching ring includes the switches or Interface Message Processors (IMPs) that perform the message assembly and disassembly functions for the access systems and perform the packet switching and control functions in routing data from origin to destination. The access ring provides the points of entry to COINS. Host computer access is through a Host Access System (HAS); terminal access (for terminals not housed on a host computer) is through a Terminal Access System (TAS); access from other networks is through a Network Access System (NAS).

Three COINS PMO DEC PDP 11/70 server host computers presently are planned: the Network Service Host (NSH), the Technology Transfer Research Facility (TTRF) computer, and the User Support Information

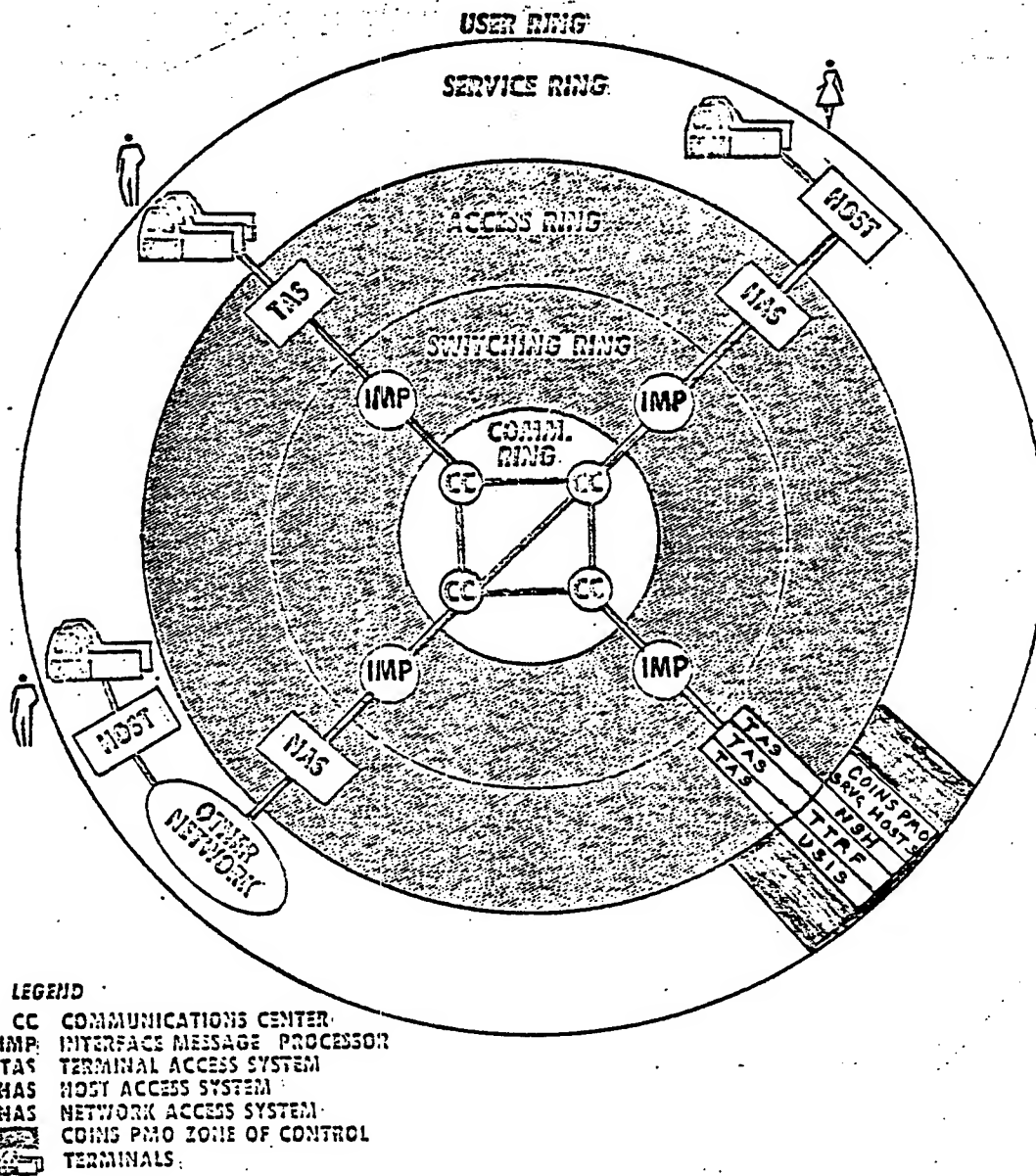


FIGURE 2

COINS PMO CONTROLLED RESOURCES

System (USIS) computer. These three service hosts are also TAs in that they will also support access to COINS from attached terminals.

In addition to the basic software for access system functions, many other COINS-provided resources are being developed to satisfy known user requirements. They include:

- ADAPT - A COINS network uniform query language to provide an alternative to using the many separate query languages of the several server hosts.
- USIS - User Support Information System, to provide on-line user training and user guides.
- NVT - Network Virtual Terminal, to provide for a wide range of terminal types to access COINS host computers without the need to implement the many terminal handler routines in the host computers.
- TCP/IP - Transmission Control Protocol/IP is the DoD standard host-to-host protocol and internet protocol.
- FTP - File Transfer Protocol, to provide an efficient way to transfer large volumes of data between host computers.
- Priority/Precedence - To provide the mechanisms to assure that the users who have the most urgent need to access COINS during crisis situations will not be locked out by less urgent usage.

By the end of FY82 the present Honeywell H316 IMP will be replaced with BBN C/30 IMPs and TAs will be installed at NAVINTCOM, DIA, Lawrence Livermore Laboratories, and State. ADAPT-II will be operational and ADAPT-III will be implemented for evaluation at the end of FY82. Also, USIS will be under evaluation and TCP will be implemented.

By FY86 NASs will be installed for the IDHSC and PLATFORM networks, a HAS will be installed for the WINDMILL host computer, a Data Base Management System will be implemented in one or more of the COINS PMO Service Hosts, ADAPT-III will be operational, USIS with a Computer Aided Instruction system will be available, TCP and NVT will be operating, and Priority/Precedence will be implemented.

4.3 COINS Network Development

Network development is, for the most part, technology transfer; i.e., evaluating existing or developing tools and techniques to determine if they would make valuable additions to the COINS. Development within COINS will occur only if a critical need exists that cannot be satisfied by adopting or adapting an existing or developing resource from outside COINS. In either instance an evaluation of the capability is made to determine its usefulness and to determine how the capability can be used or how it should be modified to make it useful.

Presently planned development activities include:

- | | |
|----------|---|
| MMRP | - Man-Machine Relationship Program, is being funded by ARPA. The COINS will be used as a test bed to evaluate the evolving hardware and software planned over the next several years. |
| RITA | - Rule-Directed Interactive Terminal Agent, is a system to develop "agents" to perform tasks for the users. The system was designed to allow for changes to be made to the agents by persons not knowledgeable in computer programming. |
| GRAPHICS | - Is a development activity to determine if computer graphics is useful, and where and how it would be useful in the COINS user community. |

Text Editing/
Word Processing - Is a development activity to determine if and where these capabilities would be useful to the COINS user community. Preparing messages for electronic mail, report (product) preparation, and preparing on-line user guides and training aids are potential applications.

Annex C is the Technical Support Plan for the COINS Network Development.

By the end of FY82 the evaluation of the electronic desk (ED-1) of the MMRP will be completed with recommendations relative to its future in the COINS community.

By FY86 a computer will be installed at one of the intelligence schools to support technology transfer and development projects and the MMRP evaluations will have been accomplished on many evolving capabilities. Also, the evaluations of RITA, GRAPHICS, and Text Editing/Word Processing will have been completed and recommendations made on if, where, and how they may be applied in the COINS user community.

4.4 COINS Network Security

COINS Network Security including need-to-know controls is concerned with adapting and developing tools, techniques, and operating procedures to ensure that the data within COINS is protected from unauthorized disclosure. The following programs have been identified as potentially useful to enhance COINS security.

KSOS - Kernelized Secure Operating System, is an approach to provide users access to a system without the need for all users to have system-high clearances. The COINS PMO is participating in the test and evaluation of KSOS.

BLACKER - Is an NSA project to provide for end-to-end encryption of data passed through a network. Initially, BLACKER is considering the user terminal to a distant host portion of the problem. Host-to-host will be accomplished later.

Multi-Jurisdiction Security Controls - Is a procedure where all users (internal and external to COINS) will be registered on a COINS Access System. The registration will include the host systems, files, and other resources for which each user has been granted access. This procedure cannot be fully implemented until all COINS access is through either a TAS, HAS, or NAS.

SNFE - Standard Secure Network Front End, is a Defense Communications Agency project to develop a standard front end for all DoD packet switched network host computers. ASDC³I has requested the COINS PMO to participate in the SNFE design and development.

User I.D. Authentication - Is the constant assessment, evaluation, and where appropriate, the implementation of techniques to authenticate legitimate users.

TAS/NAS Software Encryption - Is a project to determine how software encryption can improve security and how it should be implemented.

File/Output Labeling - Is the development of procedures to assure that files and other output is properly labeled relative to security classification and compartments.

Annex D is the Technical Support Plan for COINS Network Security.

By the end of FY82 the evaluation of KSOS, BLACKER test, and TAS/NAS Software Encryption will be completed. The COINS Access System designs of 1984 and beyond will reflect the integration of concepts embodied in BLACKER, KSOS, and other ongoing security/NTK developments. By the end of FY86 the BLACKER applications, Multi-Jurisdiction Controls, and improved File/Output Labeling will have

been implemented. The design of the SNFE will be completed and will have replaced the COINS HAS. Also, secure multi-level security access will be capable of being demonstrated.

4.5 Resource Summary

The following tables summarize the funds for the COINS PMO maintenance and development programs. The resources are shown for O&M, Procurement, and RDT&E, by Annex for fiscal years 1980 through 1986. Summary tables present the funds for O&M, Procurement, and RDT&E for fiscal years 1980 through 1986 for all annexes followed by a summary table for all funds categories for Annexes A, B, C, and D for fiscal years 1980 through 1986. The last table presents the COINS PMO staff requirements.

FUNDING SUMMARY

O&M	FY80	FY81	FY82	FY83	FY84	FY85	FY86
A	195	270	350	370	430	430	430
B	345	505	978	1,268	1,323	1,323	1,323
C	-	-	-	-	-	-	-
D	-	-	-	-	50	50	50
TOTAL	540	775	1,328	1,638	1,803	1,803	1,803

PROCUREMENT	FY80	FY81	FY82	FY83	FY84	FY85	FY86
A	--	400	--	50	--	--	--
B	746	50	1,180	75	--	--	--
C	--	--	--	--	--	--	--
D	50	80	250	300	--	--	--
TOTAL	796	530	1,430	425	--	--	--

RDT&E	FY80	FY81	FY82	FY83	FY84	FY85	FY86
A	250	150	300	520	440	390	390
B	422	400	1,299	1,405	1,100	450	200
C	--	40	50	330	430	430	430
D	135	543	535	895	600	375	205
TOTAL	807	1,133	2,134	3,150	2,570	1,645	1,225

TOTAL BY FUNDS CATEGORY

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	540	775	1,328	1,638	1,803	1,803	1,803
PROCUREMENT	796	530	1,430	425	--	--	--
RDT&E	807	1,133	2,184	3,150	2,570	1,645	1,225
GRAND TOTAL	2,143	2,438	4,942	5,213	4,373	3,448	3,028

25.6M \$ 3.6M

TOTAL BY ANNEX

ANNEX	FY80	FY81	FY82	FY83	FY84	FY85	FY86
A	445	820	650	940	870	820	820
B	1,513	955	3,457	2,748	2,423	1,773	1,523
C	--	40	50	330	430	430	430
D	185	623	785	1,195	650	425	255
TOTAL	2,143	2,438	4,942	5,213	4,373	3,448	3,028

COINS PMO STAFF (STAFF-YEARS PER YEAR)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
MANAGEMENT	8	8	9	9	9	9	9
OPERATIONS	8	11	15	15	15	15	15
USER SUPPORT	6	8	12	15	15	15	12
GRAND TOTAL	22	27	36	39	39	39	36

238 = 34/48

GLOSSARY

Following is the glossary of terms which has been developed from the combined annexes for the long range plan.

1822

BBN Report 1822, "The specification of the Interconnection of a Host and and IMP". The specification of interface between a host and the ARPANET.

Access Authorization

The permission to access a Coins element and the constraints(if any) placed on the access. Examples of constraints include the familiar access to read only, access to execute, etc. Access authorization may be placed on any COINS object, application, file, program, or device.

Access Control

The tasks imposed on a network or any of its components, performed by hardware, software, administrative controls, to control usage of the system. Included are: monitoring system operation, insuring data integrity, user identification, recording system access and changes, and granting user access.

Access Method

The technique and/or the program code in a computer, operating system that provides input/output services.

Access Time

1. The time interval between the instant at which data are called for from a storage device and the instant delivery begins.
2. The time interval between the instant at which data are requested to be stored and the instant at which storage is started.

ACK

A control bit (acknowledge) occupying no sequence space, which indicates that the acknowledgement field of this segment specifies the next sequence number the sender of this segment is expecting to receive, hence acknowledging receipt of all previous sequence numbers.

ACSI

Assistant Chief of Staff Intelligence (Army/Air Force)
Aerospace Defense Command, Colorado Springs.

ADAPT

ARPA Data Base Access and Presentation Terminal system. A common query language (UDL) being developed in phases by Logicon. Inc. It will provide (in its later phases) a common language that can be used to query any file on COINS. Adapt (Phase I) is a feasibility demonstration of the UDL to target language transforms.

ADCCP

Advanced Data Communications Control Procedure developed by ANSI. It is a bit oriented protocol.

ADP

Automatic Data Processing

ADP System Security

Includes all hardware/software functions, characteristics, and features operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities ,and

and the management constraints, physical structures ,and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system.

ADS

State Department Automated Document System.

AFIN

Air Force Intelligence, Pentagon.

AIRES

Advanced Imagery Requirements and Exploitation System.

Alternate Routing

An alternative communication path used if the normal one is not available . There may be one or more alternative paths.

Analysis

The methodical investigation of a problem, and the separation of the problem into smaller related units for further detailed study.

ANSI

American National Standards Institute.

An/Gyg-21 (V)

A digital equipment corporation (DEC) PDP-11 series minicomputer.

Application

A term used to denote a COINS data retrieval system (e.g. ISS, TIPS, SOLIS...); The object to which users are connected in processing interactive queries.(This term is deliberately chosen to make clear the separation of a host and the system(applications) now on the host. It is also intended to remind the user that a given set of hardware (a host e. g. NSH) may have two or more COINS applications (systems) (CNCC, ADAPT I, etc resident on it. Sometimes called a "system" (ISS, SOLIS); sometimes referred to by the host on which the application resides (RYE,DIAOLS).

ARPA

Advanced Research Projects Agency of the United States Department of Defense. Also DARPA.

ARPANET

The network set up by ARPA. A packet switching intercomputer network developed by ARPA. ARPANET is now managed by the Defense Communication Agency.

ARPANET Message

The unit of data transmission between a host and an IMP in the ARPANET. The maximum size is approximately 8096 bits.

ARPANET Packet

A unit of transmission used in the ARPANET between IMPS. The maximum size is approximately 1008 bits.

ASCII

American Standard code for Information Interchange. This is a seven-bit-plus parity code established by the American National Standards Institute (formerly American Standards Association) to achieve compatibility between

data services. Also called USASCII.

ASD(I)

Assistant Secretary of Defense for Intelligence, Now ASDC3I for Command Control Communications and Intelligence.

ASSIST

Army Standard System for Intelligence Support Terminals.

ATSS

Analyst Terminal Support System.

Authorization

A representation of a users right to access specific files or specific information in a file; in general the purposes for which a user has a right to access an application.

Autodin II

Automatic digital information network(Dept of Defense). This is a packet switched network scheduled to replace Autodin I in the mid-1980's.

Batch Processing

1. Pertaining to the technique of excuting a set of computer programs such that each is completed before the next program of the set is started.
2. Pertaining to the sequential input of computer programs or data.
3. Loosely, the excution of computer programs serially.

BAUD

A unit of signalling speed equal to the number of discrete conditions or signal events per second. For example, one baud equals one-half dot cycle per second in Morse code, one bit per second in a train of binary signals ,and one 3-bit value per second in a train of signals each of which can assume one of eight different states.

Binary Synchronous Communicatios (BSC)

A uniform discipline, using a defined set of control characters and control character sequences, for synchronized transmission of binary coded data between stations in a data communications system.

Birddog

A device used in Platform to do error detection and retransmission at both ends of the communication line between a directly connected "Host" or "Front End" and an IMP.

Blacker

Prototype secure communication system. A program to develop new security protection techniques on packet switched networks.

Buffer

1. A routine or storage used to compensate for a difference in rate of flow of data, or time of occurence of events, when transmitting data from one device to another.
2. An isolating circuit used to prevent a driven circuit from influencing the driving circuit.

CATENET

This term means roughly the collection of packet networks which are connected together. It is further defined as a confederation of cooperating networks.

CAI

Computer Assisted Instruction.

CAMS

Comirex Automated Management System.

Capability

Application Capability

Application Component Capability

A specification of the constraints on access. Within the range of POSSIBLE modes of access for a particular "object", if it defines what is permitted. (Note that the application and component are application-defined.)

CAS

COINS II access systems consisting of NAS, HAS, or TAS.

Channel

The logical path connecting user to hosr, or host to host. Circuits may be multiplexed to support several channels- conversely, an channel may be distributed over several circuits.

Circuit

The basic physical path over which information travels.

Circuit Switching

A method of communications where a dedicated channel or circuit between calling and called stations is established on demand for exclusive use until the connection is released. Each data path is established between two nodes by switching a data circuit for the duration of the need.

CMSS

Communication Monitoring Sub-System. (NSA Deckroof program.)

COI

Community of Interest.

CNCC

COINS Network Control Center. The installation and organization responsible for monitoring the current behavior of a network and initiating the repair of failed elements; primarily for failure reporting and accumulation of statistics.

CNMS

COINS Network Management System. A multi-faceted COINS program to develop and evaluate network usage and monitoring information.

COINS

Community on-line Intelligence System.

COINS I

This refers to the COINS Network which is continuation of the experimental COINS network that has been in operation for several years.

COINS II

COINS II is a upgraded COINS to provide needed improvements in COINS I

primarily to adapt the ARPANET packet switch technology.

COINS PMO

COINS Project Management Office

Commonality

(DOD) A quality which applies to material or systems possessing like and interchangeable characteristics enabling each to be utilized or operated and maintained by personnel trained on the others without additional specialized training; and/or having interchangeable repair parts and/or components; and applying to consumable items interchangeably equivalent without adjustment.

Communications computer

A computer that acts as the interface between another computer or terminal and a network, or a computer controlling data flow in a network.

Communications control character

A functional character intended to control or facilitate transmission over data networks. There are ten control characters specified in ASCII which form the basis for character-oriented communications control procedures. See also control character.

Compartmented Intelligence

Intelligence material having special controls indicating restrictive handling for which systems of segregation or handling are formally established.

Compatibility

(DOD) Capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interferences.

Computer Application

That portion of an application which is performed by a computer.

Computer Network

An interconnection of assemblies of computer systems, terminals and communications facilities.

Comsec

Communications Security

Connection Protocol

A procedure for establishing a communication path between two processes.

Connect time

A measure of system usage by a user, usually the time interval during which the user terminal was connected to a process in a computer, i.e. between log on and log off.

Connectivity

Basic network communication and interconnection between processes. Achieved by backbone communications network as transport facility, supporting linkage protocols (standard), and the use of standard internetwork gateways to adapt differences in network technology or protocols to support communications between processes within different networks.

CONTEXT

A teleconferencing system which is primarily devoted to document

preparation.

Control Character

1. A character whose occurrence in a particular context initiates, modifies or stops a control function.
2. In the ASCII code, any of the 32 characters in the first two columns of the standard code table. See also: Communications Control Character.

Control Procedure

The means used to control the orderly communication of information between stations on a data link.

Conversational

Pertaining to a mode of processing that involves step-by-step interaction between a computer and the user at a terminal.

Conversational mode(also interactive mode)

The interaction between a user and a specific system process in which an association, or connection, is maintained between the user and the process for the entire duration of information interchange. The duration of the connection is referred to as a "session" and the exchange of information ceases when the session is terminated.

CPU

Central Processing Unit.

Crosstalk

The unwanted energy transferred from one circuit, called the "disturbing" circuit, to another circuit, called the "disturbed" circuit.

CRT

Cathode Ray Tube

CUPA

Coins Usage and Performance Analysis.

CUSP

COINS User Support Panel.

DARPA

Defense Advanced Research Project Agency.

Data Base

1. The entire collection of information available to a computer system.
2. A structured collection of information as an entity or collection of related files treated as an entity.

Data base processing

The storage of quantities of information, in one or more forms, available to the network and its users.

Data Communications

The interchange of data from one point to another over communications channels. See Also : Data Transmissions.

Data Communication Equipment

The equipment that provides the functions required to establish, maintain and terminate a connection, the signal conversion, and coding required for communication between data terminal equipment and data circuit. The data communication equipment may or may not be an integral part of a computer; e.g., a modem.

Datagram

A packet of information which is carried to its destination without reference to any other packet, or prior establishment of a data path. An internet datagram is the unit of data exchanged between a pair of internet modules.

Data Integrity

A performance measure based on the rate of undetected errors.

Data Transmission

The sending of data from one place for reception elsewhere. Compare with DATA COMMUNICATION.

DCI

Director of Central Intelligence.

DDCMP

Digital data communications message protocol. A uniform discipline for the transmission of data between stations in a point-to-point or multi-point data communication system. The method of physical data transfer used may be parallel, serial synchronous or serial asynchronous. (DEC)

DIAOLS

Defense Intelligence Agency On-line System. Also the name of the retrieval language used on the system.

DIS

DIA Defense Intelligence School.

DOD

Department of Defense.

DOD Intelligence information system (DODIIS)

That confederation of defense organizations and activities employing manpower, automatic data processing equipment and techniques, and associated telecommunications assets which support the U. S. Defense Intelligence System.

Duplex Channel

A channel providing simultaneous transmission in both directions.

ECU

Error Correction Unit. Also referred to as BIRDDOG.

End-to-end encryption

Data encrypted at the originating node is not decrypted until it arrives at its final destination.

End to end protocol

Denotes process (on one computer) to process (on another computer) communication via virtual circuit.

EOL

A control bit (End of letter) occupying no sequence space, indicating that this segment ends a logical letter with the last data octet in the segment. If this end of letter causes a less than full buffer to be released to the user and the connection buffer size is not one octet then the end-of-letter/buffer-size adjustment to the receive sequence number must be made.

Ethernet

A high-speed communications system using a shared coaxial cable. Developed by Xerox Palo Alto Research center.

Eucom AIDES

European command Analysts Intelligence Display and Exploitation System.

FICPAC

Fleet Intelligence Center Pacific, located at Makalapa, Hawaii. n of the
Also the location of the IDHSC Pacom Switch.

Flow control (Across a connection)

The function by which a unit of data is accepted only when it can be transferred across the connection.

Frequency Division Multiplexing (FDM)

Dividing the available transmission frequency range into narrower bands each of which is used for a separate channel.

Front-End Processor (FEP)

A computer which is used to interface between a host computer and the network.

FTD

Airforce System Command Foreign Technology Division in Dayton, Ohio.

FTP

File Transfer Protocol. The protocols necessary to transmit a entire file from one host system to another.

Fundamental Protocols

Concerned with the mechanics of communication between network components. Multi-level structure for functional modularity. Isolate user level processes from communications details. Support base for the network security and network management.

Gateway

The physical and logical interface between networks. The principle function of the gateway is the transformation between protocols of different networks. In IDHSC II, the term 'Gateway' has a different meaning. Every interface to the IDHSC II ROUTER is referred to as a gateway.

H316

The Honeywell 316(a computer currently used for IMPS).

Hardware

The physical equipment or devices forming a computer and peripheral equipment.

Harmonization

(DOD) The process and /or results of adjusting differences or inconsistencies to bring significant features into agreement.

Header

The control information prefixed in a message text, e. g., source or destination code, priority, or message type.

Heterogeneous (Computer) Network

A network of dissimilar host computers , such as those of different manufacturers. At least one nodal processor has characteristics that are incompatible with those of the other nodes. Compare: Homogenous Network.

Home-Host

The host system through which a user ordinarily enters the COINS network. For many users, a TAS is their home-host; however, any computer system providing terminal user support in the COINS network is the home-host of those users "known" to it.

Homogeneous (Computer) Network

A network of similar host computers such as those of one model of one manufacturer. All nodal processors are directly compatible with regard to such characteristics as data transmission code, instruction set, and other factors which affect the ability of nodes to share data, program files, etc.

Host computer

A computer attached to a network providing primarily services such as computation, data base access or special programs or programming languages.

Host Interface

The interface between a communication processor and a host computer.

IAIPS

Integrated Automated Intelligence Processing System. IAIPS is a modernization program to integrate Navintcom systems in support of command requirements through the 1980's.

ICA

Information and Communications Applications Inc.

ICP

Initial Connection Protocol.

Identification

1. The process of providing personnel, equipment, or organizational characteristics or codes to gain access to computer programs, processes, files or data.
2. The process of determining personnel, equipment, or organizational characteristics or codes to permit access to computer programs, processes, files or data.

IDHS

Intelligence Data Handling System

IDHSC

Intelligence Data Handling Systems -Communications.

IDHSC I

The store-and-forward network managed by DIA which connects major DOD intelligence organization computer systems.

IDHSC II

The new packet switched IDHSC network which will include both batch and interactive protocol.

IIS

NPIC Integrated Information System. The original NPIC COINS host.

IMP

Interface Message Processor. The IMPS are used both as store-and-forward elements at the nodes of the communications network and as interfaces between the network and the host computers. The original IMPS were Honeywell H516 computers, slightly modified. For economy, H316 computers were later used. A microprocessor version of the IMP is under development. The new IMP is based on the BBN Microprogrammable building block(MBB). High performance PLURIBUS IMPS are also in use.

Information

1. An encompassing term including text, data, and graphic images.
2. Data organized to convey knowledge.

Information Interface

A logical interface implemented at the application, or user information, level.

Information network

A system of logically compatible information processing systems all interconnected by a communications network.

Information processing

The manipulation of information to produce the desired results.

INI

COINS Intelligence Network Interface. Front end processors used to interface the batch UNIVAC 494's at NPIC and NSA to COINS II IMP.

Initial Connection Protocol (ICP)

The official Arpanet Initial Connection Protocol as specified in NIC Document Number 7101.

INR

State Department Intelligence and Research Division Information Handling System.

Intelligence

Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies and operations.

Interactive

Pertaining to exchange of information and control between a user and a computer process, or between computer processes.

Interchangeability

(DDD) A condition which exists when two or more items possess such functional and physical characteristics as to be equivalent in performance

and durability, and one capable of being exchanged one for the other without alteration of the items themselves or of adjoining items, except for adjustment, and without selection for fit and performance.

Interconnection

(DOD) The linking together of interoperable systems.

Interface (LOGICAL)

1. Composed of a hierarchical set of protocols that are used to support communications between network processes.
2. A logical boundary between protocol layers.

Interface

1. A shared boundary defined by common physical interconnection characteristics, signal characteristics, and meanings of interchanged signals.
2. A device or equipment making possible interoperation between two systems, e.g., a hardware component or a common storage register. A physical interface.
3. A shared logical boundary between two software components.

Interface-Layer

The collection of specialized terminal access systems (TAS), COINS network front-ends, and server-hosts playing a home-host role for some users. The term arises from thinking of the network having a basic communication function (the "subnet" layer made up of the IMPS and communications lines), an interface layer (the TAS, CNAS, FE's, etc.), and a service layer (the Service hosts, Windmill, WDS, etc.).

Internetdatagram Protocol

Defines control functions required to support internetwork communications

Interoperatability

(DOD/NATU) The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.

(DOD) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.

IPC

The COINS network identifier for the Intelligence Center Pacific IDHS host computer.

IOC

Initial operational capability.y.

IP

Internet Protocol. This protocol provides a way for the TCP to send and receive variable-length segments of information enclosed in internet datagram "envelopes". The internet datagram provides a means of addressing source and destination TCPs in different networks.

ISC

CIA Information Science Center. A part of the CIA office of Training.

ISS

DIA Interactive Support System.

I/O

Input/Output

KG34

Cryptographic device.

KWS

Kiloword seconds.

Letter

A logical unit of data, in particular, the logical unit of data transmitted between processes using TCP.

LH/DH

Local Host/Distant Host IMP interfacing unit.

LHMSS

Local Host Monitoring Subsystem. One of the projects included in the COINS Network Management System(CNMS).

LINK

1. Any specified relationship between two nodes in a network.
2. A communication path between two nodes.
3. A data link. Also: Line, Circuit, Virtual Circuit.

LLL

Lawrence Livermore Laboratories.

Login (Logon)

A user access procedure to a system involving identification, access control and exchange of network information between user and system.

Logout (Logoff)

A user exit procedure from a system often providing usage statistics to the user.

Lost

The Lost system of COINS provides a measurement of the network's performance in terms of completed messages and messages that are lost.

LRP

Long Range Plan.

MBB

Microprogrammable Building Block

MBB IMP

An MBB, including I/O board and microcode or IMP I/O functions, which emulates an H316 IMP. Developed by BBN.

MCCU

AUTODIN II Multiple Channel Control Unit

Message

1. A communication mostly in words intended to be read by a person.
2. A message is a self-contained logical and physical unit of information

transmitted between a source and a destination. It may be subdivided into blocks or packets. It has a logical relevance to a source and destination. Messages are analogous to a shipment of goods where packets or blocks would represent the freight cars. Routing and other control information is contained within the message header and trailer data which is added at the origin and remains unaltered until it reaches its destination.

MITREBUS

A high speed communications system using a shared coaxial cable employing CATV technology. Developed by Mitre Corporation.

MLS

Multilevel Security.

Modem(MODulator-Demodulator)

A device that modulates and demodulates signals transmitted over communication facilities.

Module

An implementation, usually in software, of a protocol or other process.

MMRP

Man Machine Relationship Project. An ARPA sponsored program to improve human interface to computers.

MSL

Maximum Segment Lifetime, the time a TCP segment can exist in the internetwork system. Arbitrarily defined to be 2 minutes.

Multi-Level Security Mode

A mode of operation under an operating system(supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP System. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of; A) 2 or more levels of classified data, or B) 1 or more levels of classified data with unclassified data depending upon the constraints placed on the systems by the Designated Approving Authority. (Section V.C, DOD Directive 5200.28).

NAS

COINS II Network Access System. A COINS internet gateway.

HAS/FE

A host-COINS Access system.

Navintcom

Naval Intelligence Command.

NCC

Network Control Center. The installation and organization responsible for monitoring the current behavior of a network and initiating the repair of failed elements; primarily for failure reporting and accumulation of statistics. Currently the network control computer is a H316 which collects real time status information on the COINS II network.

NCP

Network Control Program. The program in a host which handles the link to the IMP and controls communications between processes in the Host and processes elsewhere in the network.

NCS

NSA National Cryptological School.

NDS

NPIC New Data System. The new NPIC COINS host.

Ned

A crt text editor developed by BBN under contract to the Rand Corporation. It is used with a CRT terminal to prepare and modify documents, letters, messages, and computer programs.

NEED TO KNOW (NTK)

An informal (up to each individual user or agency to determine the requirements for disclosure) basis for determining whether or not authorized access to information to individuals whom are otherwise properly cleared.

Network

1. An interconnected or interrelated group of nodes.
2. In connection with a disciplinary or problem oriented qualifier, the combination of material, documentation, and human resources that are united by design to achieve certain objectives, e.g., a social science network, a science information network.

Network Control Program (NCP)

That module of an operating system in a host computer, which establishes and breaks logical connections, communicating with the network on one side, and with user processes within the host computer on the other side.

Network Processing

The movement of information among information processing and data base processing components.

Network Security

The totality of measures taken to protect a network from an unauthorized access, accidental or willful interference with normal operations, or destruction. This includes protection of physical facilities, software, and personnel security. See also: PRIVACY.

Network Topology

The geometric arrangement of links and nodes of a network.

NIC

1. National Indication Center (obsolete-now merged with NMIC)>
2. Naval Intelligence Command.

NIPSSA

Naval Intelligence Processing System Support Activity.

NMIC

National Military Indications Center

NMSS

COINS Network Monitoring Subsystem. A replica of the ARPA Network Control center computer system and a component of the COINS Network

Management System. (CNMS)

Node

An end point of any branch of a network, or a junction common to two or more branches of a network.

NOSC

Naval Ocean System Center in San Diego.

NOSIC

Naval Ocean Surveillance Intelligence Center in Suitland, MD.

NPIC

National Photographic Interpretation Center

NPMO

Networks Project Management Office (NSA)>

NSASAB

NSA Scientific Advisory Board

NSH

The COINS PMO Network Service Host.

NSOC

NSA Sigint Operations Center.

NSS

NMIC Support System.

NUISS

Network Usage Information Subsystem.

Null Modem

A device which is incorporated into the line driver logic of each Coins II IMP. This device provides the NCC with the capability for remotely turning the line around to allow verification of operation.

NVT

Network Virtual Terminal. The "Standard" terminal as seen by applications on the network. Real terminals are mapped into and from the NVT.

ONI

Office of Naval Intelligence

On-Line

1. Pertaining to equipment or devices under control of the central processing unit.
2. Pertaining to a user's ability to interact with a computer.
3. Directly in the line loop. In telegraph usage, transmitting directly onto the line rather than, for example, perforating a tape for later transmission.

Open-System

The concept of openness that refers to a set of commonly agreed standards that make possible meaningful interactions between any combination of computing systems, data processing systems, or human operators which are

connected together in some way.

Operating System(O/S)

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other system related functions(Synonymous with Monitor, Executive, Control Program, and Supervisor).

Options Field

An option field may contain several options, and each option may be several octets in length. The options are used primarily in testing situations; for example, to carry timestamps. Both the Internet Protocol and TCP provide for options fields.

PAC

COINS network identifier for the IDHSC Pacom Switch.

PACOM

Pacific Command

Packet

A group of bits including data and control elements which is switched and transmitted as a composite whole. The data and control elements and possible error control information are arranged in a specified format. May be subdivisions of a message each of which may be independently routed. It is the physical container into which messages are divided for transmission.

Packet Switching

A data transmission process, utilizing addressed packets, whereby a channel is occupied only for the duration of transmission of the packet. Note: In certain data communication networks the data may be formatted into a packet or divided and then formatted into a number of packets (either by the data terminal equipment or by equipment within the network) for transmission and multiplexing purposes. This mode of operation requires an interface processor at each node of the network. An interface processor takes in a message from its host processor in segments, forms these segments into packets, and ships these packets separately to the network. The destination interface processor reassembles the packets and delivers them in sequence to the receiving system which obtains them as a single unit (message). Each packet is individually routed through the network on a dynamic routing basis toward its destination.

PACOM

Pacific Command

PACSWI

Jargon for the IDHSC PACOM switch.

PAF

COINS network identifier for the Pacific Airforce (PACAF) IDHS host system.

Parity Check

Addition of non-information bits to data, making the number of ones in each grouping of bits either always odd or always even to permit single

error detection in each group.

Password

A string of characters that is recognizable to automatic means and that permits a user access to protected storage, files, or input or output devices.

PIRL

Photo Interpreter's Retrieval Language. The retrieval language used to interrogate the NPIC COINS files that were resident on the NPIC UNIVAC 494.

Platform

A cover name for an Arpanet technology based network designed to facilitate the movement of and access to data within NSA.

PLATO

Programmed Learning and Teaching Operation. A computer-based education system developed at the Univ. of Illinois. Vended by Control Data Corp.(CDC)

PLI

Private Line Interface . Used by COINS II to encrypt data trunked through the ARPANET.

Plot 10

A general purpose graphics system.

Pluribus

High speed modular IMP. An improved IMP based on the Lockheed SUE Computer.

Privacy

The right of an individual to control the release or availability of information about himself.

Compare: Network Security.

Process

1. A systematic sequence of operations to produce a specified result,
2. A set of related procedures and data undergoing execution and manipulation by one or more computer processing units.
3. The active elements of all host computers in a network .
4. Programs in execution.

Projector

An application subsystem of Windmill which supports access to the TIPS/RYE data files.

Protocol

A formal set of conventions governing the format and relative timing of data exchange between two communicating processes. An agreement on the way in which an inter-process communication is to be processed.

Protocol Layering

The idea of layering is to insulate functions from each other, and to establish standard interfaces between functions. A layer is a set of related functions which meets 3 conditions. First, a layer must have a specific hierarchical relationship with respect to other layers. Second, it must have well defined interfaces between itself and its adjacent layers. Finally it must be able to communicate with its

peers in another host complex. Peer layers are layers in two different host complexes which perform like functions.

Real Time

A real-time computer is one whose processing time requirements are governed by external influences. It must receive data, process them, and return the results sufficiently quickly to be useful by the recipient.

Real Time System

A system performing computation during the actual time the related physical process transpires, so that the results of the computation can be used in guiding the process.

Registry Data Base

USIS files defining user profiles, user guides for COINS files, languages, and Host systems, and training courses.

Remote Job Entry

1. Submission of jobs through an input device that has access to a computer through a communications link.
2. The mode of operation that allows input of a batch job by a card reader at a remote site and receipt of the output via a line printer or card punch at a remote site. Abbr: RJE.

Response Time

The elapsed time between the generation of the last character of a message at a terminal and the receipt of the first character of the reply. It includes terminal delay, network delay, and service node delay. This is the time the system takes to react to a given input. If a message is keyed into a terminal by an operator and the reply from the computer, when it comes, is typed at the same terminal, response time may be defined as the time interval between the operator pressing the last key and the terminal typing the first letter of the reply. For different types of terminals, response time may be defined similarly. It is the interval between an event and the system's response to the event.

RITA

Rule-directed Interactive Transaction Agent previously known as Rand Intelligent Terminal Agent. A system designed for use by persons who are not computer sophisticates to develop agents (computer programs) to perform tasks in an automated fashion. It is under development by Rand and is experimentally operational.

RJE

Remote Job Entry

Routing

The assignment of the communications path by which a message or telephone call will reach its destination.

RTP

Real Time Protocol. A host-to-host protocol for communication of time critical information.

WYE/TIPS

The NSA host system housing the NSA COINS file.

SAFE

Support to the Analyst's File Environment. A joint CIA/DIA effort to develop new analyst automated support systems for both agencies.

SCCU

Autodin II Single Channel Control Unit.

SCI

Sensitive Compartmented Information.

SDI

Selective Dissemination of Information

Seawatch

NOSIC's automated ocean surveillance system.

Security Administration

The process of deciding which individuals need access to classified information to perform their duties; the verification of clearances and the entry and maintenance of the user/terminal on network and application access and authorization lists.

Security Classifications

The national classification system of Unclassified, Confidential, Secret, Top Secret.

"Server" Host

A host which makes available a resource (hardware, software or data) to other hosts or users not connected directly to itself. Note, a host can be a "user" host or a "server" host or both.

SIP

Autodin II Segment Interface Protocol.

SNCS

Secure Network Communication System. The communications network portion of CDINS II.

Software

Computer programs, procedures, rules and associated documentation concerned with the operation of computers, e.g., compilers, monitors, editors, utility programs.

SOLIS

Sigint On Line Information System.

Source

1. The point of entry of data in a network.
 2. A data terminal installation that enters into a connected channel.
- Data entry may be under operator or machine control.

Space Shuttle

A diagnostic system which is used to test network hardware and measure throughput.

Special Purpose Gateway

A gateway implementation which is not based on a standard internetwork protocol.

SSR

Air Force Standard Software Base.

Standard Internetwork Gateway

A gateway implementation which is based on a standard internetwork protocol(e.g.,TCP/IP).

Subscriber-to-Transport Protocol

Defines network interface between subscriber(host) and transport facility.

Support Programs

Programs to assist in diagnostics, testing, data generation terminal simulations, etc. are support programs.

SWI

The COINS network identifier for the Arlington Hall switch.

TAC

Autodin II Terminal Access Controller.

TAC II

Technical Assessment of the COINS II Program Ad Hoc Group of NSASAB.

TAS

COINS II Unix-based Terminal Access System.

TASMASTER

A special user who operates and maintains TAS.

T-Carrier

AT&T all-digital transmission systems available at various data rates - 1.544 mb/s (T-1), 6.312 mb/s (T-2), 45 mb/s (T-3) and 274 mb/s (T-4).

TCP

Transmission Control Protocol. A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications.

TDP

Technical Development Plan.

TEC

Toss Exchange Center.

Telenet

The ARPA Network virtual terminal protocol.

Thesaurus Data Base

Usis files containing cross reference to data values collected from various sources. These files contain data for military equipment, geographic locations, and intelligence category codes.

Tetrahedron

A secure, digital communication network in the Washington, D.C. area which utilize wideband circuits.

Text

1. Information consisting mostly of words that are readable by a person.
2. A sequence of characters forming part of a transmission which is sent from the data source to the data sink, and contains the information

to be conveyed. It may be preceded by a header and followed by an "End of Text" signal.

3. In ASCII & communications, a sequence of characters, treated as an entity if preceded by a "Start of Text" and followed by an "End of Text" control character.

THP

Autodin II Terminal-to-Host Protocol.

TILE

TIPS Interrogation Language. The retrieval language used to interrogate the NSA RYE/TIPS COINS files resident on the Univac 494.

Time Sharing

A method of operation in which a computer facility is shared by several users for different purposes at (apparently) the same time. Although the computer actually services each user in sequence, the high speed of the computer makes it appear that the users are all handled simultaneously.

TIP

Terminal Interface Processor. A Honeywell H316 computer acting both as an IMP and as a host computer to enable terminals to connect to the network without a separate Host being involved (ARPA). The TIP software is one host but other Hosts may be connected to the network via the IMP portion of the TIP.

TIPS

Technical Information Processing System. That portion of RYE/TIPS which supports the NSA COINS files.

TOCOL

Topics on COINS ON-Line.

TOSS

Terminal Oriented Support System.

Transaction Mode

The interaction between a user and the system in which no connection is established between the user and the system process which is to provide the service. The request for the service, or Transaction, is accepted by the system and forwarded to the user service which satisfies the request, the results of which are retained by the system for return to the user upon demand.

Transparent Mode

Transmission of binary data with the recognition of most control characters suppressed. In Binary Synchronous Communications, entry to and exit from the transparent mode is indicated by a sequence beginning with a special Data Link Escape (DLE) character.

Transponder

A diagnostic system which is used to test the COINS II Network Control Program and measure throughput.

Transport

The telecommunications facility which moves pieces of information from one place to another. (i.e., subnetwork, backbone, packet switching facility, etc.)

TTRF

Technology Transfer Research Facility. A facility directed by the COINS PMO to test and evaluate programs, equipment and software that may improve the service to COINS users.

Transport Protocols

Subnet protocols used between transport facility packet switch nodes to handle transmission, error detection, correction, flow control, routing.

Turnaround Time

1. The elapsed time between submission of a job to a computing center and the return of the results.
2. In communications the actual time required to reverse the direction of transmission from sender to receiver or vice versa when using a two-way alternate circuit. Time is required by line propagation effects, modem timing and computer reaction.

UDL

Uniform Data Language supported by ADAPT. The retrieval language used as the basis for ADAPT.

UNIX

Trademark for a family of computer operating systems developed at Bell Telephone Laboratories to support time sharing on the PDP 11 computers. Unix was spawned from the Multics program in the late "60s".

"User" Host

A host which support user access to a server host.

USISS

User Support Information Sub-system. (Replaced by USIS)>

Virtual Circuit (VC)

A connection between a source and a sink in a network that may be realized by different circuit configurations during transmission of a message.

Windmill

A host computer system (B7700) on the COINS II Network which supports the SOLIS and PROJECTOR (TIPS/RYE) applications. Also a host in Platform.

WMCCS

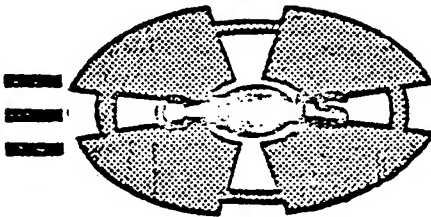
Worldwide Military Command and Control System.

Community On-Line Intelligence System

Project Management Office

National Security Agency

Fort George G. Meade, Maryland, 20755



COINS NETWORK MANAGEMENT SYSTEM

ANNEX A

TO

COINS TECHNICAL SUPPORT PLAN

Prepared by
The MITRE Corporation
7 August 1980

TABLE OF CONTENTS

	<u>Page</u>
I. DESCRIPTION	A-1
A. CNMS Components	A-1
1. The Network Monitoring Subsystem (NMSS)	A-1
2. The On-Line Network Usage Information Subsystem (NUISS)	A-5
3. COINS User Reporting Subsystem	A-5
4. The Network Control Computer (NCC)	A-6
5. Network Management Computer (NMC)	A-7
B. COINS Project Management	A-7
II. LONG-RANGE OBJECTIVES	A-9
III. JUSTIFICATIONS	A-10
IV. FACTORS BEARING ON THE PLAN	A-11
A. Facts	A-11
B. Assumptions	A-12
C. Issues	A-12
V. APPROACH	A-13
A. Network Monitoring Subsystem (NMSS)	A-13
B. Network Usage Information Subsystem (NUISS)	A-14
C. User Reporting Subsystem (URSS)	A-15
VI. STATUS AND PLANS	A-16
A. Network Monitoring Support System (NMSS)	A-16
B. Network Usage Information Subsystem (NUISS)	A-16
C. User Reporting Subsystem (URSS)	A-17

TABLE OF CONTENTS (Concluded)

	<u>Page</u>
VII. RESOURCES & SCHEDULE	A-17
A. Network Monitoring Subsystem	A-18
B. Network Usage Information Subsystem (NUISS)	A-19
C. User Reporting Subsystem	A-20
D. Total COINS Network Management System	A-20
E. COINS PMO Staffing	A-21
SCHEDULE	A-22

I. DESCRIPTION

This Annex includes 1) the COINS Network Management System (CNMS) which is perceived as a system of hardware, software, and procedures to operate, control, and manage the COINS; and 2) the human resources in the COINS PMO required to operate and manage the COINS project. COINS Project Management is presented in Section I and VII only.

The COINS Network Management System has been conceived to provide the data, processing, and display of information required to operate, control, and manage the COINS Network and its associated services. The system will support long-term management and planning as well as the day-to-day activities associated with network operations. The focal point for the CNMS data collection, processing, and display is the COINS Network Control Center (CNCC).

A. CNMS Components

Three categories of information have been identified to support the COINS Network Management: monitoring, usage, and user. The three subsystems identified to collect, process, and display the collected information are the Network Monitoring Subsystem (NMSS), the Network Usage Information Subsystem (NUISS), and the User Reporting Subsystem (URSS). Two computers, the Network Control Computer (NCC) and the Network Management Computer (NMC), have been identified to support those subsystems.

1. The Network Monitoring Subsystem (NMSS)

The Network Monitoring Subsystem (NMSS) is the part of the CNMS that coordinates and controls the network's performance activities.

The Network Monitoring Subsystem (NMSS) will collect all of the network monitoring activity into one subsystem. It includes what was formerly known as the Communications Monitoring Subsystem (CMSS), and the functions for monitoring the local hosts.

The components of the network to be monitored include:

- (1) Communications Processors (IMPs)
- (2) COINS Access Systems (CASs), i.e.,
Host Access Systems (HASs)
Terminal Access Systems (TASs)
Network Access Systems (NASs) (Gateways)
- (3) Host Processors
- (4) Communication circuits and associated equipment including COMSEC devices

The NMSS software now is a subset of the on-line Network Control Computer (NCC) software. The NCC (Honeywell 316) receives performance data from all IMPs on a timed periodic basis, and prepares status reports of communication network status that are printed on-line on the Logger Model 33 Teletype attached to the NCC. The NCC also receives diagnostic data from the network and produces reports on the Summary Model 33 Teletype attached to the NCC.

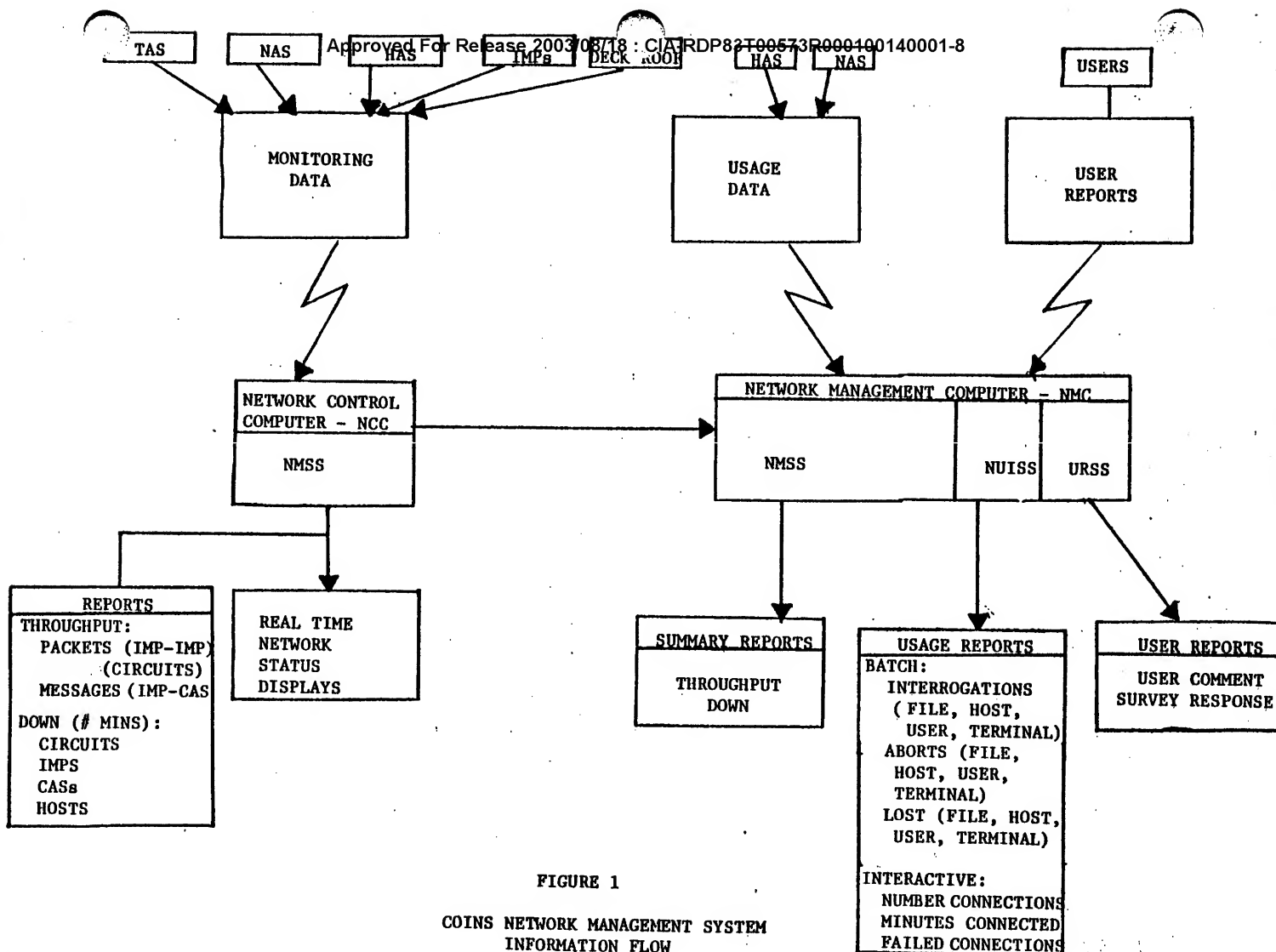
The monitoring activity, currently limited to the IMPs, will be expanded to include the COINS Access Systems, the host processors, the status of interfaced networks, and the communications. Monitoring the COINS Access Systems

will be accomplished directly with the NCC as with the DMPs. Monitoring the host processors and interfacing networks will be accomplished via the Host Access System (HAS) and the Network Access System (NAS) respectively. The communications monitoring will be accomplished through DECK ROOF.

Monitoring will include reports of throughput data as well as status reports and error reports; e.g., transmission errors, retransmissions, and unusual delays.

Figure 1 presents the general data flow for the COINS Network Management Systems.

- (a) Local host monitoring will monitor hardware, software, and communications facilities associated with a host. The monitoring will be performed in real time, identifying faults and monitoring operational thresholds so that they can be quickly evaluated and corrected as needed. The purposes of the local host monitoring activities are to keep a status on the host resources, and to detect malfunctions and to trigger corrective procedures. The local host monitor functions will be accomplished by the NCC and Host Access System. Findings will be reported to the local host manager and to the COINS Network Control Center.
- (b) Communication Monitoring - DECK ROOF (or a successor) will be installed in COINS to monitor the T1 (TETRAHEDRON) network and COMSEC devices.



The design includes provision for special monitoring information to be provided to the NMSS (on an exception basis) of any COINS-related malfunctions or other significant events.

DECK ROOF was started in response to a requirement from the COINS PMO to NSA/T to develop a real-time capability to monitor all T1 communications facilities associated with COINS II and report problems. The project was expanded by NSA/T to include the monitoring of all NSA communications facilities including COINS.

2. The On-Line Network Usage Information Subsystem (NUISS)

The On-Line Network Usage Information Subsystem (NUISS) collects and integrates system logs for each host and switch and tabulates information on usage, operating performance, responsiveness, and reliability of COINS.

3. COINS User Reporting Subsystem

The COINS User Reporting Subsystem will provide the mechanisms for users, managers, and system personnel to comment on their experiences with the COINS Network and its accessible resources, to suggest changes to the network and accessible resources, or to suggest new capabilities and services.

Included in the design concept is a mechanism to assure that all comments and suggestions are responded to by the responsible organizations.

Another facet of the design concept is to support general and selective surveys to solicit comments. These surveys will be conducted by the COINS PMO but the impetus for such surveys may be provided by any organization related to the COINS Network.

4. The Network Control Computer (NCC)

The Network Control Computer (NCC) supports remote diagnosis and software maintenance. Diagnostic and statistical data from each of the IMPs are automatically reported to the NCC approximately every minute. When network degradation is reported, background programs can retain control of the network, isolate equipment failures from communications line trouble, and perform many kinds of recovery. From the Network Control Center, it is possible to reload IMP software throughout the entire network. It also performs and coordinates troubleshooting activities in COINS. At present, the NCC operators use three different consoles to perform their operations and control functions. It is planned to automate these functions while operating from one console.

The obsolete NCC H316 Computer will be replaced by a BBN C/70 Processor.¹ At the time of the C/70 implementation,

¹The C/70 is a processor based on the BBN Microprogrammable Building Block (MBB) architecture. The BBN C/30, also called the MBB IMP, will replace the H316 IMPs.

extensions to the monitoring system will be initiated to cover all COINS Network major components. Also, the monitoring data will be transferred to the NMC for maintaining a history file, developing trends, and providing management reports. Concurrently with the BBN C/70 installation, all network operations, diagnostics, tests, and corrective action- will be accomplished at a single integrated console. The console will include CRT displays (graphic and alphanumeric) as well as hardcopy output.

5. Network Management Computer (NMC)

With the upgrading of the NCC Computer, a second BBN C/70 processor will be installed to process the monitoring and throughput information, to collect and process the usage data in support of NUISS, and to collect, process, and retain information in support of the User Reporting Subsystem. The NMC will also be used to develop, test, validate, and verify software for the NCC and NMC and will function as a backup for the NCC.

B. COINS Project Management

COINS project management is described as management, operations, and user support.

The management activities are:

- Program Planning and Budgeting
- Contracting and Contract Monitoring
- Inter-Agency Coordination

Identifying User Requirements
Configuration Management
Serving on Various Community Committees and
Ad Hoc Working Groups
Developing, Implementing, and Monitoring
Appropriate Security Procedures

The management activities are expected to change little in the next five years and, therefore, the management staff will remain relatively static.

The operations activities are:

Operate and Arrange for Maintenance of the Equipment Located in the CNCC: IMPs, NCC, NMC, NSH, TTRF, and associated peripheral devices.

Identify and Correct Network Faults.

Maintain Accurate Status of the COINS Network and its Components.

Coordinate Error Detection and Correction with Other COINS Participants.

Maintain Physical Security of CNCC.

Validate and Verify New or New Releases of Network Software and Hardware.

Develop Procedures for All Aspects of Operations.

The COINS Network is now operating 17 hours per day (0600-2300) Monday through Friday excluding holidays. It is planned to increase the operations staff and to extend the period of operations to 24 hours per day, seven days a week including holidays.

The user support activities are:

Develop Training Courses.

Conduct Training Courses

Assist Users in Accessing COINS Resources

Determine Courses for User Problems and Taking
Corrective Actions

Informing Users of New and Changed Resources
and User Guides

Coordinating Training Requirements with
Participating Agencies

With the addition of new users brought about by the increased accessibility of COINS through TASs, new host computers (DODIIS) and interfacing networks, the work load on the user support will increase dramatically over the next two-three years. The situation will be worsened with the addition of new hosts and their attendant resources and different methods and procedures. The situation will change little until 1986 when person-to-person training will give way to the automated User Support Information System using Computer Aided Instruction (e.g., CDC PLATO). It is expected that the user support staff can be reduced at that time.

II. LONG-RANGE OBJECTIVES

The goal of the CNMS is to provide timely accurate information in a useful form to network managers: to perform the day-to-day management of the network, to maintain a data base of performance and usage data for trend analysis for short- and long-range planning of qualitative and quantitative improvements, and to detect degenerating conditions in the network.

The long-range objective is to develop and implement a fully automated on-line system for the collecting, editing, analyzing, and

reporting network information. This information will be used by the COINS PMO to monitor the network operations and performance, and to assess the utility of the COINS II Network to the end users of the COINS accessible services. Subsets of the information will be provided to the agencies involved with the COINS PMO for their information, evaluation, and action, and to support their resource management and budgeting decisions. Further, it is an objective to automatically perform fault diagnosis and fault correction to the maximum extent practical.

It is recognized that this objective will not be achieved in a single giant step but rather will be achieved gradually over the years. It is also recognized that while incremental improvements are being defined, developed, tested and implemented, existing procedures and methods must be maintained in an operational status.

III. JUSTIFICATIONS

Management is a priori requirement for a system as valuable and complex as the COINS network. The network is both complex in its operations and in the development of capabilities to satisfy the users' needs. To eliminate or at least minimize the false or misdirected starts in satisfying user needs, monitoring the qualitative aspects of COINS accessible services is just as important as the quantitative aspects. Timely and accurate information about the network, its accessible services and user satisfactions is required to do the cost-benefit analysis necessary to allocate scarce resources to improve existing services, to increase capacity of existing services, and to provide new services.

Failure to collect the needed information to present it in usable form, to analyze it, or to act on the acquired knowledge will result in the deterioration of the existing services, ignoring user needs by not improving or developing capabilities, or by providing inappropriate capabilities or inappropriate changes.

The development program for the CNMS is in direct response to the ASD(I) Review Group Report on the Evaluation of the COINS Experiment dated 1 February 1973. The review group recommended that:

"Present COINS reporting procedures be modified to allow the collection of statistics more amenable to permitting evaluation of system usage, timeliness, and effectiveness. The COINS Project Manager should be directed to submit a plan for statistical reporting which would (a) identify the objectives of such reporting (i.e., what must be learned about the system), (b) the items of data to be collected to satisfy the objectives, and (c) the analysis to be performed on the data to provide the desired information."

IV. FACTORS BEARING ON THE PLAN

A. Facts

1. Most of the service host computers are not owned by the COINS PMO and, therefore, are not under the COINS PMO control. As an alternative to the host reporting status data every n seconds (the preferred mode), the local host status data will be derived by sending appropriate messages to the host system and evaluating the responses. These monitoring activities will be accomplished by the NCC and the Host Access Systems and preclude the need to modify the host computer system to support COINS monitoring. A similar procedure may have to be adapted for interfacing networks.

2. With regard to the monitoring of the TETRAHEDRON network and COMSEC devices which are being monitored by the DECK ROOF system currently under development, the NMSS must content itself with that data which will be made available by these developers and managers of DECK ROOF.

B. Assumptions

1. It is assumed that the DECK ROOF manager will provide the data necessary for NMSS to operate, control, isolate malfunctioning components, and to inform users and managers of outages or pending outages of all COINS major network components. If this assumption proves false, a complete status of the COINS Network may not be available and will reduce the fault isolation ability of the CNCC.

2. It is assumed that the DODIIS hosts attached to the COINS Network will be attached, monitored, and require the collection of usage data the same as COINS hosts. If these host computers are to be treated differently, the difference must be known to reflect them in the design of the CNMS. See ISSUES, paragraph IV.C. following.

C. Issues

The COINS Network has been designated (at least informally) by DIA to be the Washington, D.C. area network for DODIIS. As such, the DODIIS hosts in the area will be attached to the COINS Network in the same fashion as COINS hosts; i.e., through a Host Access System. It is not known at this time if the CNMS will be required to collect,

process and store the same type of information for the DODIIS host systems as is planned for the COINS hosts. Also, it is not known how many DODIIS hosts will be attached to COINS.

If this issue is not resolved, a choice must be made relative to how to treat the DODIIS hosts in the subsystems - the choice may be wrong necessitating redesign and reprogramming.

V. APPROACH

The approach to meeting the long term objectives of the CNMS will be evolutionary because current systems and procedures must be maintained in an operational mode as new hardware, software and procedures are developed and implemented.

A. Network Monitoring Subsystem (NMSS)

With the delivery and installation check out of the NCC BBN C/70, the IMP monitoring functions now accomplished by the H316 will be converted to the BBN C/70. Following the H316 to C/70 conversion, the monitoring will be extended to include the COINS Access Systems (HAS, NAS & TAS) and the server hosts that are attached to COINS with a Host Access System. Concurrently, arrangements will be made with DECK ROOF system to send communication and COMSEC status data to the NCC for integration with other network status data.

Monitoring and throughput data collected by the NCC will be passed to the Network Management Computer (NMC) for storage and for analyses to determine if chronic problems exist or are developing in any of the components, and to support trend analysis

of the components and sets of components. In the ARPANET, processing of historical (longer than most recent 24 hours) monitoring data is accomplished in the DEC PDP 10 computer at BBN. These processes were never implemented in the COINS Network because of a shortage of computer resources. With the installation of the BBN C/70 as the NMC, the processing of historical monitoring data and traffic data will be initiated on the COINS Network. Also, the monitoring and traffic data will be correlated with usage data to determine if poor performance on any set of major components show positive correlation exists between usage and poor performance in order to determine and implement appropriate corrections.

B. Network Usage Information Subsystem (NUISS)

The first step in the evolution of the NUISS has been started, i.e., the network usage information processing is being moved from the IBM 370 system (not a COINS host) to the COINS Network Service Host (NSH), PDP 11/70. The system logs are still processed on the IBM 370, but some of the files extracted from the logs are manually transferred to the NSH to prepare the reports needed by the COINS PMO.

This migration will continue until all processing is accomplished on the NSH including the initial processing of the system logs. It is anticipated that all NUISS processing will be accomplished on the COINS NSH by the end of FY 1981.

The feasibility of collecting the system logs automatically from the COINS access systems has been demonstrated. The capability will be implemented as the network hosts adopt the COINS II Host Access System (HAS) as their network interface. This transition will be completed by 1984.

Concurrently with the IBM 370 to NSH migration and implementation of automatic log collection, a BBN C/70 micro-programmable processor will be installed (end FY81) to perform the collection, processing, storage and display for the CNMS including the NUISS. Beginning in FY82, the processing for NUISS being done on the NSH will migrate to the BBN C/70 NMCS computer. The software development for processing NUISS data on the NSH will be compatible with the BBN C/70 and can be transferred with little difficulty after the C/70 has been installed and checked out.

C. User Reporting Subsystem (URSS)

The User Reporting Subsystem does not exist in any structured way in COINS. A pilot system will be implemented during FY81 to evaluate the concept, establish the design characteristics of such a system, and to determine how it should be implemented. Assuming the pilot system evaluation results in a decision to provide a User Reporting Subsystem, an initial capability will be developed and implemented on the CNMC BBN C/70 starting in FY83.

VI. STATUS AND PLANS

A. Network Monitoring Support System (NMSS)

Network monitoring is presently maintaining the status quo - no development effort is ongoing. A capability specification is being prepared for extending the monitoring to the COINS Access Systems and the server host computers. Current plans call for BBN to design and program the extensions for the BBN C/70, and to deliver the monitoring software with the hardware late in FY81. Likewise, a capability specification for the processing of network monitoring data comparable to the capabilities provided by the DEC PDP 10 computer at the BBN ARPANET Control Center, will be presented to BBN so that the software to process historical status and traffic data will be delivered with the BBN C/70 late in FY81.

Enhancements to the NMSS will be developed in FY82 through FY84 to provide the host monitoring functions and further enhancements if experience indicates their need.

B. Network Usage Information Subsystem (NUISS)

The processing of two major files, CUPA and LOST, have been transferred from the non-COINS UNIVAC 494 (RYE/TIPS) to the COINS Network Service Host (NSH). The host computer logs are collected manually and processed to extract the CUPA and LOST files which are then manually transported to the NSH where management reports are prepared and displayed for information and action.

The next step is to move the processing of the manually collected system logs to the NSH where they can be merged with automatically collected system logs from the COINS Access Systems. This processing of manually collected logs and implementation of the automatic collection of the CASS system logs will be accomplished as the server host computers convert to using the COINS Host Access System (HAS). The conversion is planned for completion when WINDMILL attaches to a HAS in FY84. In FY82, the NUISS will be transferred from the NSH to the NMC.

During FY82 and FY83, the NUISS management reports will be refined and expanded to take advantage of available graphics capabilities available on the Network Service Host.

During FY84, the processing will be developed to correlate usage data with monitoring data.

C. User Reporting Subsystem (URSS)

The pilot User Reporting Subsystem will be implemented in one or two Terminal Access Systems (TASs) in FY81 and be system evaluated throughout FY81 and into FY82. A capability specification for the URSS will be developed in FY82 and the system will be developed for the BBN C/70 in FY83 and implemented starting in FY84.

VII. RESOURCES & SCHEDULE

The following tables show the funds that have been budgeted or programmed and, for the out years, planned to develop, implement and

maintain the COINS Network Management System. The funds are those required for procurement and contractor support. In-house resources are excluded.

A. Network Monitoring Subsystem (NMSS)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	175	170	250	250	250	250	250
Procurement	---	400	---	50	---	---	---
RDT&E	---	---	200	200	200	150	150
TOTAL	175	570	450	500	450	400	400
1000 of Dollars							

The FY80 and FY81 O&M funds are those required to maintain the hardware and software for the existing NCC H316. The O&M funds for FY82 through FY86 are to maintain the hardware and software for the NCC BBN C/70 and the NMC BBN C/70.

The FY83 procurement funds are to purchase a console for the integrated display of monitoring data in the CNCC.

The procurement funds (FY81) are for the purchase of two BBN C/70 hardware and the network monitoring software for the NCC C/70, and the software to process the historical monitoring data for the NMC C/70. The RDT&E funds in FY83 through FY86 will support enhancements to the NMSS, develop software for the CNCC integrated display, and to develop automated diagnostic and

fault correction routines and to develop validation and verification software for the CNCC. The RDT&E funds in FY82 are to develop software for correlating monitoring and usage data on the NMC.

B. Network Usage Information Subsystem (NUISS)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	20	100	100	120	120	120	120
Procurement	---	---	---	---	---	---	---
RDT&E	250	150	100	120	120	120	120
TOTAL	270	250	200	240	240	240	240
1000 of Dollars							

The O&M funds are to maintain the software for the NUISS. The RDT&E funds for FY80 and FY81 are to transfer the NUISS processing from the IBM 370 to the COINS Network Service Host (NSH) PDP 11/70 and to implement the automatic collection of system logs from COINS Access System. RDT&E funds in FY82 will support the transfer of NUISS from the NSH to the COINS Network Management Computer (CNMC), BBN C/70. RDT&E funds for FY84 through FY86 will be for the development of reaction reporting on a real-time basis.

C. User Reporting Subsystem (URSS)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	---	---	---	---	60	60	60
Procurement	---	---	---	---	---	---	---
RDT&E	---	*	*	200	120	120	120
TOTAL	---	---	---	200	180	180	180
1000 of Dollars							

* The development of a pilot URSS will be accomplished under the Man Machine Relationship Program which is funded by the DOD Advanced Research Project Agency (ARPA). See Annex C, Network Development.

The RDT&E funds (FY83-FY86) are to develop, implement, and enhance the operational URSS following the pilot system evaluation.

D. Total COINS Network Management System (CNMS)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	195	270	350	370	430	430	430
Procurement	---	400	---	50	---	---	---
RDT&E	250	150	300	520	440	390	390
TOTAL	445	820	650	940	970	820	820
1000 of Dollars							

E. COINS PMO Staffing

The resources for the COINS PMO are shown in terms of the in-house staff requirements rather than dollar resources.

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
Management	8	8	9	9	9	9	9
Operation	8	11	15	15	15	15	15
User Support	6	8	12	15	15	15	12
TOTAL	22	27	36	39	39	39	36
Staff Years per Year							

SCHEDULE

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
<u>NMSS</u>							
• Install 2 BBN C/70s		▲					
• Test Hardware and Software for NCC & NMC		▲					
• Develop Correlation Routine for Monitoring and Usage Data			▲				
• Develop Enhancements for NCC & NMC			▲				
				▲	▲	▲	▲
<u>NUISS</u>							
• Transfer Processing to NSH PDP 11/70		▲					
• Implement Automatic Log Collection	▲	▲	▲	▲	▲		
• Transfer Processing from NSH to NMC BBN C/70			▲				
• Develop NUISS Enhancements			▲	▲	▲	▲	▲
<u>URSS</u>							
• Develop Pilot URSS		▲					
• Evaluate Pilot URSS			▲				
• Develop Operational URSS					▲	▲	▲



Community On-Line Intelligence System

Project Management Office

National Security Agency

Fort George G. Meade, Maryland, 20755



COINS NETWORK RESOURCES

ANNEX B

TO

COINS TECHNICAL SUPPORT PLAN

Prepared by
The MITRE Corporation
7 August 1980

TABLE OF CONTENTS

	<u>Page</u>
I. DESCRIPTION	B-1
A. Interface Message Processors (IMPs)	B-3
B. Host Interfaces	B-4
C. COINS Access System (CAS)	B-4
D. ADAPT	B-4
E. User Support Information System (USIS)	B-5
F. Other User Services	B-6
II. LONG-RANGE OBJECTIVES	B-6
A. Interface Message Processor (IMPs)	B-7
B. COINS Access System (CAS)	B-7
C. Service Host	B-8
D. ADAPT	B-9
E. User Support Information Systems (USIS)	B-9
F. New Protocols	B-10
G. Network Virtual Terminal (NVT)	B-11
H. Priority/Precedence	B-12
III. JUSTIFICATION	B-12
IV. FACTORS BEARING ON THE PLAN	B-14
A. Factual	B-14
B. Assumptions	B-15
C. Issues	B-16
V. APPROACH	B-16
A. Interface Message Processors (IMPs)	B-17
B. COINS Access Systems (CASs)	B-18
C. Service Hosts	B-20
D. ADAPT	B-21
E. User Support Information System (USIS)	B-22
F. New Protocols	B-22
G. Network Virtual Terminal (NVT)	B-24
H. Priority/Precedence	B-25
VI. STATUS AND PLANS	B-25
A. Interface Message Processors (IMPs)	B-26
B. COINS Access Systems	B-26
C. ADAPT II	B-27

TABLE OF CONTENTS (Concluded)

	<u>Page</u>
VI. STATUS AND PLANS (Continued)	
D. User Support Information System (USIS)	B-27
E. Network Service Host (NSH)	B-28
F. New Protocols	B-28
G. Network Virtual Terminal (NVT)	B-29
H. Priority/Precedence	B-30
VII. RESOURCES AND SCHEDULE	B-31
A. Interface Message Processor (IMP)	B-31
B. COINS Access Systems (CASs)	B-32
C. ADAPT	B-33
D. User Support Information System (USIS)	B-34
E. Network Service Host (NSH)	B-34
F. New Protocols	B-35
G. Network Virtual Terminal (NVT)	B-36
H. Priority/Precedence	B-36
I. Total COINS Network Resources	B-37
SCHEDULE	B-38

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	Current COINS Host Computer Interface	B-2

I. DESCRIPTION

Resources as used here include the hardware and software that are provided to the servers and users of COINS by the COINS PMO. Included are the Interface Message Processors (IMPs), the interfaces between the IMPs and host computers, the Terminal Access Systems (TASs), the interfaces to other networks, and the software resident in the suite of hardware.

Presently the interfaces between the IMPs and host computers consist of an Intelligent Network Interface (INI) for the RYE system at NSA, a Front End Processor (FEP) for the SIGINT On-Line Information System (SOLIS) at NSA and a Host Access System (HAS) for the New Data System (NDS) at NPIC. See Figure 1. The INI and FEP use DEC PDP 11/40 computers with the ELF operating system. The HAS uses a DEC PDP 11/70 computer with the UNIX operating system. It is planned that all host computer interfaces will be standardized on the DEC PDP 11/70 UNIX HAS architecture when the WINDMILL computer assumes the RYE and SOLIS functions.

In addition to the preceding hardware, the COINS PMO provides Private Line Interfaces (PLIs) to allow the use of ARPANET as a backbone communications network to gain access to the COINS network. A PLI is installed at IPAC and one has been purchased and is scheduled for Lawrence Livermore Laboratories (LLL) in FY81.

The communications lines--TETRAHEDRON in Washington, D.C. area and leased or ARPANET elsewhere--are not provided by the COINS PMO. The hard wire communication between IMPs and TASs, and between IMPs and host computer interfaces are provided by the COINS PMO.

SYSTEM	HOST COMPUTER	NAME	<u>INTERFACE</u>	
			HARDWARE	OPERATING SYSTEM
RYE	U-494	INI	PDP 11/40	ELF
SOLIS	B 7700	FEP	PDP 11/40	ELF
NDS	U 1110	HAS	PDP 11/70	UNIX

FIGURE 1

CURRENT COINS HOST COMPUTER INTERFACE

The software provided and maintained by COINS PMO includes those programs resident in the front ends, access systems, IMPs, and PLIs that implement the basic services of those hardware devices and programs to provide special services directly to the users. These special services as envisioned today include a common query language (presently ADAPT), a User Support Information System (USIS), a text editor, a data base management system to provide a home for data files of community interest that cannot be made available on another COINS host computer, mail and message services, teleconferencing, local personal file storage, and data manipulation capabilities.

Some of these may be resident in one or more COINS host computers. Others may be made available in COINS Access Systems, or COINS PMO sponsored host computers. Notable among the latter is the User Support Information System. A host computer to adopt homeless files could be provided by the COINS PMO or another participating agency if unused capacity were available on the host.

Following are brief descriptions of the COINS PMO provided hardware and software resources.

A. Interface Message Processors (IMPs)

The IMPs are the packet switches to interconnect the host computer and COINS Access Systems on the COINS network. The IMPs are owned and controlled by the COINS PMO as are the programs residing in the IMPs.

B. Host Interfaces

The Intelligent Network Interface (INI) and a Front-End Processor (FEP)—both DEC PDP 11/40s with the ELF operating system—serve as the COINS Network interface for the NSA RYE and SOLIS systems respectively. The INI and FEP will be replaced with a COINS Host Access System (HAS) when the WINDMILL computer takes over the RYE computer functions. At that time, WINDMILL will house both RYE and SOLIS systems.

C. COINS Access System (CAS)

The CAS is an umbrella name for Host Access System (HAS) which is the interface between a host computer and COINS, Terminal Access System (TAS) which is the interface between terminals and COINS, and Network Access System (NAS) which is the interface (gateway) between another network and COINS.

The CASs and most of the resident programs are provided and controlled by the COINS PMO. All TAS software is under COINS PMO control, all HAS software including that part required to interface with the host computer is controlled by the COINS PMO, and the COINS half of the NAS is controlled by the COINS PMO.

D. ADAPT

ADAPT eliminates the requirement for users to learn and use the query language for each host computer system they have need to access by providing a common query language. The common query language is transformed into the query language of the host computer being accessed and prepares the query response

for display to the user. The user has the option to use the standard language or the target system language. Batch and interactive modes are available through ADAPT.

E. User Support Information System (USIS)

USIS is the central automated repository of all information concerning the resources on COINS that are available for users, and how these resources can be used. All user guides for files, query languages, and other resources (e.g., USIS, ADAPT, Text Editors, and host computers) will be available in USIS and accessible via COINS for training and user reference.

The key characteristics of USIS are user profiles, guides and training aids, authoring and a thesaurus. User profiles record, for each registered user, areas of interest relative to the resources available via COINS. The profiles are used to automatically inform the users of changes in various guides. The guides are the many on-line publications that provide information for accessing and using the available resources. The training aids provide sample uses (sample queries for example) of the resources, and provide lesson plans for training the user not familiar with a particular resource. Authoring provides the mechanisms for the responsible individuals to prepare the user guides on-line. The mechanisms are constructed such that the format of guides are standardized and, therefore, easier to understand when many guides must be learned. The thesaurus provides a cross reference of data element names and codes as they

are used in the many files of the sponsoring agencies. The thesaurus in this regard is an interim measure to alleviate the problems brought about by the lack of data element standardization.

F. Other User Services

One or more text editors will provide the users with the capability to prepare and modify documents on-line. This capability, coupled with mail and teleconferencing, facilitates coordination and collaboration when the originators of an intelligence product must coordinate or collaborate with geographically dispersed participants. Using the COINS Network for product production is more efficient than the mails or travel.

Local, personal file storage and data manipulation capabilities provided needed services to users who access COINS through a TAS and must rely on COINS accessible resources for all such services.

II. LONG RANGE OBJECTIVES

The long range objectives are to provide the servers and users needed hardware and software support that is more cost-effective for COINS PMO to provide than another member organization. Further, the COINS PMO will endeavor to supply these resources in such a way so as to encourage the use of the valuable resources accessible on the COINS Network.

The sponsoring agencies are encouraged to provide and maintain resources for COINS users when it is more cost-effective than can be

achieved by the COINS PMO. The provision of text editing, for example, may be better provided by all agency host computers and made available to COINS users who need the service. However, no plans exist for the COINS member agencies to extend text editing or other services, except for processing and responding to file queries, to users via the COINS Network. Many resources will be supplied by the COINS PMO because many COINS users access the host computers via TASs and the only computer resident resources available to them are those offered on the COINS Network.

To achieve the long range objective of cost-effective support, the COINS PMO plans to provide standardized access system hardware and standardized protocols for gaining access to any resource available via COINS. Standardization will lead to cost-efficiency in resource acquisition and maintenance. A single access command language will allow a user to access any COINS resource.

A. Interface Message Processor (IMPs)

The IMPs will be upgraded from the current Honeywell H316 processors to the new BBN C/30 microprogrammable processor. The current H316 processors are obsolete and are becoming more difficult and more costly to maintain. Software for the IMPs will be centrally maintained in the COINS Network Control Center and will be downstream loaded to the IMPs.

B. COINS Access System (CAS)

The network interfaces now being used for RYE and SOLIS at NSA and the IDHSC gateway at DIA will be replaced by Host Access

Systems and a Network Access System respectively. Standardizing the COINS access also makes possible a common mechanism to control access to the COINS network and available resources.

The long range plan for the COINS CAS is to limit their functionality (where practical) to providing and controlling access to the COINS Network. All CASs—Host Access (HAS), Terminal Access (TAS), and Network Access (NAS) will provide for bilateral communications between their respective components, for access controls required for COINS Network security and for a precedence/priority system for use when the COINS Network or an accessible resource becomes overburdened. The COINS PMO plans to achieve and maintain uniformity of the COINS Access Systems and to provide and control the CASs and the software—for which the COINS PMO is responsible—for accomplishing the functions of the CASs.

Uniformity of hardware and software will minimize the cost of software development and maintenance and provide for downstream loading of software from the COINS Network Control Center. Uniformity is necessary for maintaining configuration control over the software resident in the CASs.

C. Service Host

The COINS PMO service host computers in the long term will be attached to the network in the same fashion as other agency host computers; i.e., with a HAS. Where practical, the services now supported by the TAS that are required to support users who

enter the network via a TAS will be moved to one or more COINS PMO service host computers or the service host computers of other participating organizations.

The COINS PMO Network Service Host (NSH) currently installed on the COINS Network is being used for COINS PMO purposes--software development, TAS backup, software testing, and processing usage information. When the BBN C/70 processor takes over usage data processing and the User Information Support System (USIS) is moved to a USIS dedicated PDP 11/70 (end of FY82), the NSH will be used to supply services for users.

D. ADAPT

The development of ADAPT to provide a uniform information retrieval language is aimed at eliminating barriers to the use of the information available on the many COINS host computers that result from the need to learn many retrieval languages. ADAPT will go through incremental improvement cycles based on user experience with each successive revision of ADAPT.

E. User Support Information System (USIS)

USIS will, in the long term, become part of a computer-aided instruction system to provide COINS users with high quality instruction at their home work stations. At that time it is expected that the courseware for COINS users will be prepared by professional instructors who are knowledgeable in the resources being covered. The instructors of the several intelligence

schools are likely candidates for courseware development. The COINS PMO will be responsible for developing instruction programs to teach how the COINS Network is accessed and to teach the users how to use any unique services that are provided by the COINS PMO.

The CAI version of USIS will maintain records of student achievements to measure the students' progress and to provide information for use in evaluating the effectiveness of the lessons and instructional material.

F. New Protocols

The ASD(C³I) has directed all DoD computer networks based on the packet switch technology to adapt the standard DoD Transmission Control Protocol (TCP) for host-to-host communication and the standard Internet Control Protocol (IP) for communications between computer networks. The COINS PMO plans to adopt these protocols after they are evaluated in a test bed environment to determine the impact they may have on throughput and to determine if other software should be modified to minimize any detrimental impact that the protocols may have.

The need for a general File Transfer Protocol (FTP) will be investigated and if one is needed, it will be adapted from an existing FTP or a new one developed for implementation in COINS. The purpose of the FTP is to provide a mechanism for effective and efficient large volume data transfers from a host

to another host or to an access system that provides file services. The purpose of an FTP is not to provide for replicating files or large sections of files on various processors to satisfy users desires to have their private data bases. Clearly, this would defeat the reason for COINS inception; i.e., sharing information that is maintained by the single agency responsible for the completeness, accuracy, and timeliness of the information.

G. Network Virtual Terminal (NVT)

The COINS PMO will implement a Network Virtual Terminal to provide for handling a wide range of user terminals on the network. The NVT will translate the individual terminal characteristics into the NVT representations at the processor closest to the terminal (e.g., TAS) and will translate from the NVT representation to the individual user terminal characteristics. At the server end of the communication (e.g., HAS) the NVT representation will be translated into terminal characteristics of a terminal type that is serviced by the host computer system and vice versa. Using the NVT protocols, a wide range of terminal types can be used for accessing COINS resources without the need for each host to implement terminal handling software for each type of terminal.

H. Priority/Precedence

A priority/precedence system will be implemented in COINS to assure that users involved in crisis situations are given the best possible service within the COINS. Presently, all users have equal priority and precedence whether they be trainees or NMIC Watch Officers.

The priority/precedence system will be implemented in the COINS Access Systems (CASs). In this way all network access to all resources on COINS can be controlled, however, the COINS priority/precedence system cannot govern user access that is made directly to the host computer.

III. JUSTIFICATION

The provision of the capabilities to share intelligence information among the users within the intelligence community is the keystone of the COINS charter. These basic capabilities (resources) are provided through an assemblage of Interface Message Processors (IMPs), the communications between the IMPs, COINS Access Systems, and the procedures and software needed for their proper functioning.

To this basic set, resources of community interest have been added to support the efficient exchange and processing of information, and to provide a system for COINS user support. The need for these resources is not the consequence of a single agency's action, but is the consequence of all participating agencies collectively. For this reason, the User Support Information System and ADAPT are being

developed to address the global problems of COINS user training and the multiple query languages respectively. Likewise, a file transfer protocol, network virtual terminal, and priority/precedence are network-wide solutions to problems that are brought about (at least in part) by the network.

A network-wide mail/message service and teleconferencing can be implemented in the several host computers, the COINS Access Systems or some of both. Implementation in the COINS Access Systems is planned whether or not they are implemented elsewhere. It will be less costly because the services need only be developed once and replicated in the standard access systems. Implementation in the several host computers, even if all affected agencies agreed, would require separate development, implementation and maintenance for each host.

Further, the COINS PMO has provided and is planning on expanding, services to users who access COINS via a TAS. The storage, processing, manipulation, and display of retrieved information for this group of users is limited to the services provided on COINS by the COINS PMO or to those that can be accomplished manually, unless the hardcopy of the retrieved data is entered into another computer available to the user that can process Top Secret SCI information. Since some COINS users who have need to access, retrieve, and process intelligence data are members of agencies outside the intelligence community and the Department of Defense, COINS is the only source for automated storage and processing of retrieved classified data.

Justification for the provision of a host computer and DEMS to make available data files of community interest that cannot be made available on another COINS host is dependent on the number of such files and the amount of interest in accessing the data. COINS PMO will only provide this service if the number of files and amount of interest justify their COINS accessibility, and no other COINS host has excess capacity.

IV. FACTORS BEARING ON THE PLAN

A. Factual

1. DIA has indicated that the COINS will be the Washington, D.C. area network for DODIIS. This will require a Host Access System for each DODIIS computer to be attached to COINS. The number of such hosts have not been determined, and therefore, program planning and budgeting cannot be accomplished. Also, it is not known to what extent the DODIIS system guides, file guides, etc. must be included in USIS.
2. During the transition of IDHSC to AUTODIN II, a gateway between IDHSC and AUTODIN II will not be developed. COINS will provide the communication link for AUTODIN II subscribers to access IDHSC hosts and vice versa. COINS must provide sufficient capacity at both gateways to handle the traffic until the transition of IDHSC to AUTODIN II is completed.

3. The Network Control Protocol (NCP) currently being used in COINS will be replaced with the DoD standard Transmission Control Protocol (TCP4), and the DoD standard Internet Protocol (IP) will be implemented in COINS. The impact of these changes must be assessed to determine if other COINS software must be modified to accommodate the new protocols and maintain efficient operations. Initial indications are that a different version of the UNIX operating system may be required by the COINS Access Systems—TASs, HASs, and NASs. Also, the NCP of the ELF operating system based INI and FEP will not be changed to TCP4. A method must be developed to allow the coexistence of NCP and TCP4/IP in COINS.

4. There is no precedence/priority system in COINS. In the event of a crisis resulting in a heavy load on one or more COINS resource or host computer, there is no mechanism whereby the users who have the critical need for service can be given preferential treatment.

B. Assumptions

1. The DODIIS computers to be attached to COINS will be COINS hosts; i.e., be interfaced with a COINS Host Access System and use the COINS protocols. See paragraph IV A.1., preceding. If these hosts are not interfaced via a HAS or other protocols are implemented, special arrangements must be made for their attachment to COINS.

2. Users who access the COINS from a TAS will require COINS-provided special services for the storage, processing, and display of retrieved data. Also, services provided for universal use that can be provided more cost-effectively by COINS will be developed and implemented by the COINS PMO.

If this assumption is false, development programs and contracts must be curtailed depending on the inaccuracy of the assumption.

C. Issues

The number of DODIIS hosts to be attached to COINS is not known. The number of hosts and the schedule for joining COINS must be established in order to plan, program, and budget for the hardware and software acquisition. The delay in establishing the number and schedule could result in unacceptable delays in attaching the hosts to COINS and delay the transition of IDHSC to AUTODIN II.

V. APPROACH

The approach to meet the long term objectives of the COINS PMO is to evolve modularized hardware and software for the IMPs, COINS Access Systems, and COINS PMO Service hosts so that functions may be changed, added or deleted on any component easily with minimum impact on the component and other components in the network. The functional

description of the COINS presented in Part II, COINS Architecture, will provide the basis for modularization.

This approach will provide for the addition, modification or deletion of functions on a universal basis (e.g., all access systems), a subset (e.g., all terminal access systems), or on a single component (one access system). In this way components can be tailored to meet specific requirements without sacrificing the advantages of standardization.

As mentioned, the approach is evolutionary, and probably will not be completely implemented until the end of the 1980's. To accomplish the degree of modularity required, hardware and software must be implemented whose architecture is supportive of modular implementations of the required functions.

A. Interface Message Processors (IMPs)

The functionality of the IMPs has remained static since the packet switching technology was adapted for COINS. There are no plans to change the functions being performed by the IMPs. The Honeywell H316 processors will be replaced by BBN C/30 processors. The BBN C/30 is the smallest system available in the BBN micro-programmable Building Block line of computer systems. If the functions assigned to the IMP were increased, the C/30 capacity and capability could be easily enhanced to accommodate the increase.

B. COINS Access Systems (CASSs)

Of all the components of COINS, the COINS Access Systems will benefit most from a modular/functional approach to accomplish the delivery of COINS network services. The Terminal Access System (TAS) as presently configured, is a relatively large DEC PDP 11/70 system at approximately \$250,000 per copy for hardware. The number of TASs will increase from two to six over the next two years and perhaps more in later years, but no firm projections have been made. The current TAS is configured to provide many services beyond those required for terminal access and its configuration does not easily support tailoring each TAS to the needs of the organizations and individual users. Ideally, each service (or perhaps logical subset) would be maintained in a standard configuration and provided to those access systems that have need for it. Likewise, any special hardware for a service would need to be part of the TAS only if the service was installed. The general purpose hardware, e.g., memory and processing power and terminal ports, would be sized for each TAS installation. The modular approach to network services will provide for structuring a minimum TAS (hardware and software) when only terminal access support is needed, and will provide for a TAS that looks more like a service host, if such is required, without losing control of the configuration of the hardware and software and still take advantage of reduced costs afforded by standard hardware and software acquisition and maintenance.

Even if hardware cost becomes an insignificant part of the total cost, a functional modular approach to the hardware and software architecture will minimize the impact of software changes in one function on other functions, and will facilitate the changing of software to firmware and vice versa when desirable.

The same advantages apply to the Host Access Systems (HASs) and Network Access Systems (NASs), but perhaps not to the same extent. To date, only one HAS has been installed and, although a gateway exists between IDHSC and COINS, it is not a COINS standard. With such little experience, the functions that may be optional for a HAS or NAS cannot be known with much confidence. In some instances, however, a HAS may also provide for terminals to access the COINS network through the HAS. This will require some of the TAS services and hardware to be installed in the HAS.

Similar situations may prevail with the NAS. It is expected that the need for a modular NAS will be clear if the envisioned local office networks with wide variations in their capabilities and protocols are attached to COINS via NASs. Some with a rich assortment of services will use a minimal NAS, with others the NAS may be the best location to provide needed services normally associated with a TAS.

The NAS design in total requires collaboration with the gateway designers of the other network. It is not clear if the COINS PMO should be responsible for developing software to

translate from COINS to what is expected by the other network or to translate from other into COINS, do both or neither. The assigned responsibilities (to COINS PMO and other networks) will most likely be different for different networks.

The first steps in the evolution to a modular architecture for hardware and software will be to upgrade all COINS host interfaces to standard Host Access Systems, to provide a functional description of the NAS, and to develop a design for the COINS half of the system. Many functions (at least at the less detailed levels) for all access systems are the same; for example, access control, monitoring and usage reporting. For this reason, a functional description of each access system will be prepared in order to select a single hardware architecture to satisfy all COINS Access Systems.

Once an architecture has been established and the basic design is developed, suppliers can be identified to provide the standardized, modular hardware and software.

Further, if the downward trend of hardware cost continues, the implementation of redundant CASs will be considered to improve reliability especially for hosts access systems and network access systems.

C. Service Hosts

The implementation of the User Support Information System (USIS) on a dedicated computer in FY82 and the transfer of the Network Usage Information Subsystem (NUISS) to the Network

Management Computer in FY82, the Network Service Host (NSH) will be free to offer services to users. The NSH will initially provide the capabilities for users to keep personal files and perform text editing functions on the personal files. As a follow-on, a Data Base Management System (DBMS) will be installed on the NSH for local file retrieval and data manipulations.

In addition to the NSH, the installation of the CIA RECON host will provide for implementing files of community interest that are sponsored by agencies that do not sponsor a host on COINS. It is expected that the CIA RECON host will be installed in FY85 although a schedule has not been established.

D. ADAPT

ADAPT II will be ready for evaluation beginning in FY81. It will be installed on one or more TASs for use by the persons supported by the TAS and by COINS PMO personnel. The evaluation is expected to be done over a 12-month period. During the evaluation, minor changes will be made to enhance the utility of ADAPT II.

During the evaluation a specification will be prepared for ADAPT III based on user experience with ADAPT II and identified additional capabilities. ADAPT II will continue to be used in an operational environment during the development of ADAPT III which will be evaluated in a fashion similar to ADAPT II.

E. User Support Information System (USIS)

A USIS pilot system will be installed on DEC PDP 11/70 computer in the COINS PMO. The pilot system will be used during FY81 to assess its benefits and to develop a specification for a production model of USIS (USIS-I), assuming that the USIS benefits can justify the cost of its development. The development of the production model will take place during FY82 and FY83.

USIS-I will not include an on-line computer-aided instructional (CAI) system. The incorporation of USIS into a CAI system will be considered during the USIS-I evaluation when a suitable CAI system can be identified for use on the COINS Network. At this time, it is not clear if USIS will be complemented by a relatively simple CAI system or if USIS will become one application on a highly sophisticated system such as PLATO.

F. New Protocols

1. Transmission Control Protocol and Internet Control Protocol (TCP/IP)

The first step in adapting the DoD Standard TCP/IP is to develop a test bed to assess the impact of the new protocols on the throughput on the COINS Access Systems, and to identify any needed changes in other CAS resident software--notably the UNIX operating system.

Concurrently with the design of the test bed, the throughput of the present Network Control Protocol (NCP)

access systems will be benchmarked to provide a basis for the impact analysis.

During FY81, tests will be run with TCP/IP and the version of UNIX presently being used in the COINS Access Systems to make throughput measurements and to identify any bottlenecks. The tests will be repeated with modifications in UNIX or other access system software to determine to what extent the throughput can be increased and the bottlenecks can be eliminated.

Assuming acceptable throughput can be achieved, the TCP/IP protocols will be installed in the COINS Access Systems in the latter part of FY81.

Associated with the TCP/IP impact analysis and installation are an impact analysis using TCP/IP and the Kernel Secure Operating System (KSOS), and the development of a mechanism to provide for the coexistence of NCP and TCP in the COINS. These activities are presented in Annex C, COINS Network Development Summary.

2. File Transfer Protocol (FTP)

A study will be performed to determine the requirements for an FTP. There is no recognized need for an FTP to support users of COINS in the current mode of operations for COINS; i.e., query-response activity. However, the DODIIS hosts to be added to COINS may have need to transfer large amounts of information to other DODIIS hosts. Also as COINS evolves to provide services beyond query-response, an FTP may be required.

An FTP is now operating in COINS, but it is limited to transfer between DEC PDP 11 processors. If the study reveals a need for an FTP for other COINS hosts, either an existing FTP (ARPANET FTP for example) or a new FTP will be developed.

G. Network Virtual Terminal (NVT)

The different types of terminals that should be accommodated by the NVT and the characteristics of the NVT and where the translations from real terminal to virtual terminal and vice versa are under study.

It is planned at present to implement COINS NVT in the UNIX based COINS Access Systems. Implementation of NVT for all hosts then will not be completed until the WINDMILL computer uses a Host Access System to connect to COINS - now scheduled for mid-FY1984. NVT could be implemented in TASs and the Host Access System for NDS to provide a richer assortment of terminals to access NDS. However, the TAS terminals (other than TTY Model 40) could not access RYE, SOLIS or DIOALS because the NVT would not be recognized by the front ends or gateway respectively. This limited increase in flexibility for TAS users will not justify starting the development of a COINS NVT.

The specification development for a COINS NVT will be undertaken in FY83 with a phased implementation starting in the second half of FY84. By FY83, NVT developments for networks to which COINS will interface (PLATFORM and AUTODIN II for example) should be far enough along so that the COINS development can take advantage of the ongoing or completed developments. Also, the COINS NVT translation requirements for other network NVTs will be known.

H. Priority/Precedence

The priority/precedence system will be defined for COINS after similar systems resident on the other networks with which COINS will interface are studied and evaluated. To the extent that the COINS system differs from others, a translation must be made at the gateways for the other networks. The problems that may exist in assuring uniform treatment when multiple networks are involved in the source-destination channel are not known. The procedures for the priority/precedence system will be spelled out and coordinated with all agencies involved before the system is designed and implemented.

The system will be implemented in the COINS Access Systems. This will assure uniform treatment within COINS and will not involve the host systems in the system development and implementation. Also, the system need be developed once and replicated in all standard COINS Access Systems.

VI. STATUS AND PLANS

The status of the COINS Network Services range from completely operational to undefined. COINS-II is an operational network and has completely replaced the central switch of COINS I. All traffic within COINS is now passed via one or more IMPs from origination to destination.

The ARPANET-COINS interface experiment to determine the feasibility of using the ARPANET as the long haul communications net between PACOM and COINS is still considered to be in a test phase. PACOM, however, is using the connection to submit queries and receive responses in support of their operational needs.

The same techniques that are employed in the PACOM-COINS test will be implemented to give Lawrence Livermore Laboratories (LLL) access to COINS in an operational mode. The LLL access is scheduled for mid-FY81.

A. Interface Message Processors (IMPs)

The Honeywell H316 IMPs will be replaced by the BBN C/30 processors starting in mid-FY81 and phased to the end of FY83. A BBN C/30 has been installed in the COINS network and was shown to be plug-to-plug compatible with the H316.

Five H316 COINS IMPs are now operating—one at DIA, one at NPIC, one at NSA, and two at the COINS PMO, plus the BBN C/30 in the COINS PMO. In addition to replacing the H316 IMPs, two new C/30 IMPs will be installed in mid-FY81—one at NAVINTCOM and one at the State Department to support TASSs.

B. COINS Access Systems

The COINS Terminal Access System (TAS) has been operational since FY78. Three TASSs are now operating—one at PACOM and two at the COINS PMO. During FY81, four more TASSs will be installed—one each at NAVINTCOM, State Department, DIA, and LLL in that order.

Presently, one COINS Host Access System (HAS) is installed at NPIC to interface the NDS to COINS. The second HAS will be procured in FY82 and will be installed for the WINDMILL computer at NSA in FY84.

Three COINS Network Access Systems (NASSs) are planned for interfacing the IDHSC, AUTODIN II, and PLATFORM networks to COINS. The IDHSC and PLATFORM NASSs are planned for implementation in early FY84. Implementation of the NAS to interface AUTODIN II and IAIPS to COINS has not been scheduled.

C. ADAPT II

ADAPT I was developed to demonstrate the feasibility of the approach taken to address the multi-retrieval problem.

ADAPT II is being developed and will be installed in early FY81. Following its installation the system will be evaluated relative to the user interface, the utility of provided capabilities to users, and the efficiency of operation.

Based on this evaluation a specification will be prepared during FY81 for development of ADAPT III during FY82. ADAPT III is planned for delivery at the beginning of FY83 and will be evaluated during FY83.

D. User Support Information System (USIS)

The pilot USIS will be implemented on COINS PMO DEC PDP 11/70 at the end of FY80. An evaluation program to be undertaken during FY81 will culminate in a specification for USIS-I, which will be developed during FY82 and FY83. An investigation will be started in FY83 to determine if a computer-aided instruction (CAI) system would be a useful, cost-effective adjunct to USIS. If it is

determined that a CAI system should support USIS, a development effort to incorporate USIS in a CAI system will be undertaken in FY84.

E. Network Service Host (NSH)

The PDP 11/70 currently designated as a network service host has been used to develop software and to support the COINS Network Management System (Annex A), and it will continue in these roles through FY82. Beginning in FY83, the PDP 11/70 will be available to support users with an editing capability and provide for the storage of user files. These services can be supported by software currently available on the PDP 11/70.

In FY83 a Data Base Management System (DBMS) will be selected and installed on the network service host. The selection will be based on an evaluation of how well the DBMS that are available for PDP 11 systems satisfy the perceived needs of the users to be supported and the cost of acquisition and maintenance.

F. New Protocols

1. Transmission Control Protocol and Internet Control Protocol (TCP/IP)

The study to determine any detrimental effects of implementing the DoD standard TCP/IP in the UNIX based COINS Access System will be undertaken in FY81. The effort will start in FY80 with the preparation of a test bed design and a plan for accomplishing the study.

Assuming no major problems are encountered during the study, TCP will be implemented in the UNIX based Access System in FY82.

If major problems are discovered, implementation will be delayed until the problems are solved. The delay will be determined by the nature of the problems and availability of resources to address them.

2. File Transfer Protocol (FTP)

A file transfer protocol, furnished by DEC for PDP 11 computers, is being used by COINS to transfer system logs from the COINS Access Systems to the NSH computer. This FTP is only usable between two PDP 11 systems.

The study to determine the need for a general FTP will be undertaken in FY83. If the study shows a generalized FTP is needed, a survey of available FTPs will be made to determine if an existing FTP can be used by COINS or adapted for COINS. If an FTP must be developed for COINS, it will take place in FY84.

G. Network Virtual Terminal (NVT)

An interim report on an NVT study was completed in November 1979. This study estimated the cost for developing a highly flexible NVT would range from \$1.8 million to \$2.7 million. Because an NVT would not be of significant value to COINS users until all resources were accessible using an NVT, the start of

and NVT program will be delayed until FY83. It is expected that other NVT developments now planned or in progress will be usable, at least in part, and will reduce the cost of a COINS NVT significantly. Also, the NVTs now being considered for IDHSC, AUTODIN II, and PLATFORM, will be firm enough to provide a firm specification for translating between the COINS NVT and other network NVTs.

In FY83 the NVT for COINS TASS and HASS will be specified. The development effort will take place in FY83 and FY84. Implementation will be accomplished by the end of FY85.

The NVT for COINS Network Access Systems (NASS) will be included in the designs for those gateways. The design for the IDHSC and PLATFORM NASS will start in FY83 and be implemented in FY84. The AUTODIN II NAS design is not scheduled.

Presently, the TTY Model 40 teletype is a de facto NVT in the COINS Network. The Delta Data terminals on NDS and other types of terminals on the NSH are made to appear as TTY Model 40 when they enter the COINS Network. The same approach is being taken for the HP 2645 terminals at NAVINTCOM.

H. Priority/Precedence

The study of the priority/precedence systems used in the network that will interface COINS (AUTODIN II, IDHSC, and IAIPS) will take place in FY83. The functional description of the COINS priority/precedence system and the procedures for when the system will be invoked, treating traffic reaching COINS or in COINS, and treating the priorities/precedences of the interfacing networks will be prepared in FY83.

The procedures will be coordinated with all agencies participating in COINS (users and servers) early in FY84. In anticipation of only minor changes during coordination, a design specification for the system will be developed concurrently with the coordination. Development of the system will be completed and implemented early in FY85.

VII. RESOURCES AND SCHEDULE

The following tables show the funds that have been budgeted, programmed or planned to procure, develop, implement, and maintain the hardware and software associated with the COINS Network Resources.

The funds shown are those required for procurement and for contractor support. In-house resources are shown in Annex A, COINS Network Management System.

A. Interface Message Processor (IMP)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	85	85	165	165	165	165	165
PROCUREMENT	--	50	100	50	--	--	--
RDT&E	--	--	--	--	--	--	--
TOTAL	85	135	265	215	165	165	165
1000 of Dollars							

The O&M funds are for the hardware and software maintenance of the present H316 IMPs in FY80, FY81 and FY82 and to maintain the BBN C/30 IMPs starting in FY81 and continuing through FY86.

The procurement funds, FY81-FY83, are for the purchase of five BBN C/30 processors and their resident software. Not shown is the acquisition of two or three BBN C/30 IMPs to be provided by the PLATFORM project in exchange for a COINS PMO owned BBN PLURIBUS IMP.

B. COINS Access Systems (CASs)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	260	420	813	1,078	1,078	1,078	1,078
PROCUREMENT	746 ¹	--	780 ²	--	--	--	--
RDT&E	123	100	874	500	250	--	--
TOTAL	1,129	520	2,467	1,578	1,328	1,078	1,078
1000 of Dollars							

Except for \$28,000 in FY80 to upgrade the existing COINS PMO TAS, the O&M funds are for hardware and software maintenance for Terminal Access Systems (TASs), Host Access Systems (HASs), and Network Access Systems (NASs). In FY80 three TASs, and one HAS are covered. Three additional TASs will be purchased in FY80 and maintained starting in FY81. The TAS at LLL will be maintained under a separate LLL contract. The funds for maintaining the NAVINTCOM TAS will be transferred to COINS PMO via MIPR. Increases in FY82 and FY83 are for two NASs and two HASs that will be added to the maintenance requirements through FY86.

¹\$296 provided by COINS PMO; \$225 provided by NAVINTCOM for one TAS; \$225 provided by LLL for one TAS.

²Includes funding for the purchase of: HAS for WINDMILL, NAS for PLATFORM, and a NAS for IDHSC.

The procurement funds in FY80 are for existing COINS PMO TAS upgrade (\$71,000), for purchasing three TASs (\$675,000) in FY80, and for purchasing two NASs and two HASs in FY82. The funds for the purchase of the LLL TAS and NAVINTCOM TAS will be transferred to the COINS PMO via MIPRs by the respective organizations.

The RDT&E funds for FY80 and FY81 are for software enhancements to TAS and HAS software. The FY82 funds are for development of NAS software for the PLATFORM and IDHSC NASs and HAS software for the WINDMILL and CIA Host HASs. The NAS and HAS software development will continue into FY83. Also included in FY82 and FY83 are funds for expected CAS software enhancements. All FY84 funds are to develop expected CAS software enhancements.

C. ADAPT

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	—	—	—	25	25	25	25
PROCUREMENT	—	—	—	—	—	—	—
RDT&E	123	150	150	50	0	0	0
TOTAL	123	150	150	75	25	25	25
1000 of Dollars							

The RDT&E funds in FY80 are for the development and implementation of ADAPT II. FY81 RDT&E funds will provide for the evaluation of ADAPT II, minor enhancements to ADAPT II and preparation of the ADAPT II specification. FY82 funds are to be used for developing ADAPT III which will be evaluated using FY83 funds.

Maintenance of ADAPT is planned to commence in FY83.

D. User Support Information System (USIS)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	50	50	50
PROCUREMENT	--	--	300	--	--	--	--
RDT&E	96	50	250	300	250	200	100
TOTAL	96	50	550	300	300	250	150
1000 of Dollars							

The RDT&E funds budgeted in FY80 will provide a USIS Pilot system that will be evaluated in FY80. FY82 and FY83 RDT&E funds will be used to develop USIS I. Also in FY83, the feasibility of complementing USIS with a Computer Aided Instruction (CAI) system will be determined. Assuming a USIS/CAI system is desirable, it will be developed in FY84 and FY85. Funds for USIS enhancements are planned in FY85 and FY86.

Contractor maintenance for USIS will start in FY84. Purchase of the USIS Host Computer System will take place in FY82.

E. Network Service Host (NSH)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	5	5	5
PROCUREMENT	--	--	--	25	--	--	--
RDT&E	--	--	--	10	--	--	--
TOTAL				35	5	5	5
1000 of Dollars							

The O&M procurement and RDT&E funds are for the selection acquisition and implementation and maintenance of a data base management system for the COINS PMO network service host.

F. New Protocols

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M							
PROCUREMENT							
RDT&E	*80	100	25	45	150	—	—
TOTAL	80	100	25	45	150		
1000 of Dollars							

*Funds provided by ASDC3(I)

The study to determine any detrimental impact of replacing the Network Control Protocol (NCP) with TCP in the COINS Access Systems will start in FY80 and be completed in FY81. Assuming the replacement of NCP with TCP is desirable, it will be implemented in extant COINS Access Systems in FY81 and FY82. COINS Access Systems acquired after FY81 will have TCP.

The RDT&E funds in FY83 are to determine the requirement for a FTP to survey existing protocols and to select and adapt an existing FTP for COINS. In the event a new FTP must be developed, the FY84 funds will be required.

G. Network Virtual Terminal (NVT)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M							
PROCUREMENT							
RDT&E				350	250	200	100
TOTAL				350	250	200	100
1000 of Dollars							

Development on NVT for COINS is planned to start in FY83 with a Phase 1 operational capability to be implemented by the end of FY84. A second version of NVT will be undertaken in FY85 and implemented in FY86.

Installation of NVT will be limited to COINS Access Systems, and, the maintenance of NVT is included in the O&M funding plan for the COINS Access Systems.

H. Priority/Precedence

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M							
PROCUREMENT							
RDT&E				150	200	50	
TOTALS				150	200	50	
1000 of Dollars							

The RDT&E funds cover the study of the other network systems, developing procedures, and the design and implementation of the COINS priority/precedence system. Since the system will be installed in the CASS, O&M funds for maintenance are included in the CAS funding.

I. Total COINS Network Resources

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	345	505	978	1268	1323	1323	1323
PROCUREMENT	746 ¹	50	1180	75	—	—	—
RDT&E	422	400	1299	1405	1100	450	200
TOTALS	1513	955	3457	2748	2423	1773	1523
1000 of Dollars							

¹\$296 provided by COINS PMO for one TAS; \$225 provided by NAVINTCOM for one TAS; \$225 provided by LLL for one TAS.

SCHEDULE

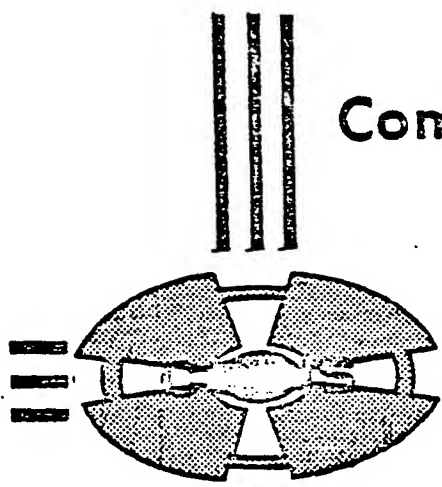
	FY80	FY81	FY82	FY83	FY84	FY85	FY86
<u>IMP</u>							
• Purchase BBN C/30		▲	▲	▲			
• Install BBN C/30							
NAVINTCOM		▲					
State Dept.		▲					
• Replace H316 with C/30			▲	▲			
<u>CAS</u>							
• Purchase 3 TASs	▲						
• Install TASs							
NAVINTCOM		▲					
DIA		▲					
LLL		▲					
State Dept.		▲					
• Install TAS Enhancements	▲	▲	▲				
• Purchase 1 HAS and 2 NASs			▲				
• Develop HAS and NAS Software				▲			
• Implement Software for:							
PLATFORM NAS				▲			
IDHSC NAS					▲		
WINDMILL HAS					▲		
• Install CAS Enhancements			▲	▲	▲	▲	▲
<u>NSH</u>							
• Select DBMS				▲			
• Implement DBMS				▲			

SCHEDULE (Continued)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
<u>ADAPT</u>							
• Develop & Implement ADAPT II	▲						
• Evaluate ADAPT II		▲					
• Prepare Specifications for ADAPT III		▲					
• Develop & Implement ADAPT III			▲				
• Evaluate ADAPT III				▲			
<u>USIS</u>							
• Develop & Implement Pilot USIS	▲						
• Evaluate Pilot USIS		▲					
• Develop USIS			▲				
• Implement USIS				▲			
• Evaluate CAI				▲			
• Develop USIS/CAI					▲		
• Implement USIS/CAI						▲	
<u>NEW PROTOCOLS</u>							
• Define TCP Test Bed	▲						
• Evaluate TCP		▲					
• Implement TCP			▲				
• Determine FTP Requirements				▲			
• Adapt FTP for COINS				▲			
<u>NVT</u>							
• Develop NVT				▲			
• Implement NVT					▲		

SCHEDULE (Concluded)

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
<u>NVT (Cont'd)</u>							
• Enhance NVT						●	▲
• Implement Enhanced NVT							●
							▲
<u>PRIORITY/PRECEDENCE</u>							
• Study Other Systems			●	▲			
• Develop Procedures				●	▲		
• Coordinate Procedures					●	▲	
• Prepare Specification					●	▲	
• Develop System						●	▲
• Implement System						●	▲



Community On-Line Intelligence System

Project Management Office

National Security Agency

Fort George G. Meade, Maryland, 20755

COINS NETWORK DEVELOPMENT

ANNEX C

TO

COINS TECHNICAL SUPPORT PLAN

Prepared by
The MITRE Corporation
7 August 1980

TABLE OF CONTENTS

	<u>Page</u>
I. DESCRIPTION	C-1
II. LONG-RANGE OBJECTIVES	C-3
III. JUSTIFICATION	C-3
IV. FACTORS BEARING ON THE PLAN	C-5
A. Facts	C-5
B. Assumptions	C-6
C. Issues	C-7
V. APPROACH	C-8
A. General Procedure	C-9
B. Net Development	C-10
C. Training Management	C-12
VI. STATUS AND PLANS	C-12
VII. RESOURCES AND SCHEDULES	C-14
A. Man-Machine Relationship Program (MMRP)	C-14
B. RITA	C-15
C. TEXT EDITING/WORD PROCESSING (NED)	C-15
D. GRAPHICS	C-15
E. ADAPT, MMRP AND RITA INTEGRATION	C-15
F. TOTAL NETWORK DEVELOPMENT	C-16
SCHEDULE	17
APPENDIX: CAPABILITIES FOR EVALUATION	18

I. DESCRIPTION

This annex provides the long-range plans for new development, evaluation, and testing of hardware and software necessary to provide and maintain high quality COINS services so that users will be encouraged to exploit the COINS accessible resources.

The COINS PMO is not responsible for building better mouse traps, but for providing accessible easy-to-use paths to the door. In this regard the COINS PMO will continue to remove or reduce the barriers that exist between the information stores and the users' capability to make full use of the information. Many of these barriers have been described in Section I, COINS Concept of Operations, and Section II, COINS Architecture. Notable are the need to use many retrieval languages and the shortage of automated user tools to store, manipulate and otherwise process information from many sources after retrieval. Ways to remove or reduce these barriers is the object of COINS network development activities.

The main thrust of COINS network development is technology transfer. The COINS PMO looks to existing capabilities or capabilities being developed (and funded) by other organizations and evaluate them to determine if they can be adopted or adapted for use in COINS. Paramount of the technology transfer approach was the adaptation of ARPANET packet switching technology to COINS in order to improve the poor network performance and to decrease the vulnerability associated with the central store and forward switch that preceded packet switching in COINS. Technology transfer continues in many other areas.

The development (COINS funding) route is chosen only when no other acquisition of the capability is satisfactory and the need for the resulting capability justifies the higher acquisition cost. Major among the developments are the COINS Access Systems—TAS, HAS, and NAS.

In addition to the development and the evaluations associated with technology transfer, network development includes the testing of developed or modified capabilities prior to their achieving operational status in COINS.

To support the COINS Network Development, test beds are needed for new development, evaluation, and testing. These test beds consist of general and special purpose hardware and software, and must be tailored to support the capability involved in the activity. The amalgam of these test beds is called the Technology Transfer and Research Facility (TTRF). The TTRF will be a dynamic facility—changing, growing, and shrinking depending on the activities being supported. It may contain many test beds at one time, and a test bed may be geographically distributed; i.e., the TTRF is not constrained to a single location.

Although TTRF is primarily a research, test and evaluation facility, the technology transfer functions require extensive training of users who will participate in the testing and evaluation of the new capabilities. To provide for realistic test and to accomplish the necessary training, the TTRF must provide terminal access to the COINS network and associated host computers. For this reason,

it lends itself well for use as the main training facility to access the User Support Information System (USIS) to indoctrinate potential users of COINS and to train them in how to use the operational capabilities and data available via the COINS network. The use of the TTRF to support operational training will require only a small part of the computer and terminal time, and in many instances both research and training support can take place simultaneously. Using the TTRF to support operational training, therefore, will not adversely affect its primary function.

II. LONG-RANGE OBJECTIVES

The long-range objectives of the COINS Network Development are little, if any, different from the short term. The continuous assessment of the quality and quantity of COINS-provided services as described in Annex A, COINS Network Management System, will identify areas where more efficient or more effective support should be provided to COINS users. Resource constraints as well as other external influences will dictate a priority for undertaking network improvements. The long-range objectives then are to provide as many needed improved or additional services as are possible within the constraints.

The TTRF long-range objective is to locate at a TTRF computer at one (or more) of the intelligence schools (DIS, ISC or NCS) and provide terminal access to it from the other schools. In this way the schools can participate extensively (if desired) in the evaluation of new tools and techniques, and also have access to USIS and all other COINS accessible resources for operational training.

III. JUSTIFICATION

The network development activities are required to improve and maintain the effectiveness of COINS in supporting the users of its accessible resources. These activities include the adoption, adaption or development of needed hardware and software capabilities, the test and evaluation of new or new releases of software and user training.

The ASD(C³I) has directed all DoD packet switched networks to adopt the DoD standard Transmission Control Protocol and the Internet Control Protocol (TCP/IP). It is necessary to identify any adverse affects TCP/IP may have on the performance of the COINS Access Systems. The performance measurements will be made in the COINS Technology Transfer Research Facility.

The justification for technology transfer stems from the belief that it is more cost-effective to adapt hardware and software for the COINS community of users than it is to expend resources on development of capabilities to satisfy perceived needs.

Some capabilities are, and will be, the result of research projects funded by the DoD. The technology transfer research activities provide vehicles not only to determine if operational capabilities are useful in the COINS community, but provide vehicles to influence development to improve the probability that a final piece of hardware or software package will be a cost-effective addition to the COINS-provided services. The ADAPT system, which provides a uniform data language interface to multiple query languages, and the Man-Machine Relationship Program

(MMRP) are two examples of projects initiated by the DoD Advanced Projects Research Agency (DARPA) that are, or will be, using the COINS community via the TTRF to evaluate the prototype editions of the capabilities.

This synergistic relationship provides DARPA with evaluations of the fruits of their efforts in an operational or operational-like environment and provides the COINS PMO with the opportunity to influence further developments.

The funding for the development of the Kernelized Secure Operating System (KSOS) was arranged by ASD(C³I). KSOS was developed to run on the DEC PDP-11 computer and emulates the UNIX operating system. The PDP-11 with the UNIX operating system is the base for the COINS Access System. Because of this and the potential of KSOS to improve COINS security, ASD(C³I) and COINS PMO have agreed to use the COINS Technology Transfer Research Facility to construct a test bed to evaluate the security features of KSOS and to do performance measurements on KSOS based COINS Access Systems.

Within the TTRF is a COINS-II Terminal Access System (TAS) that will be complemented from time to time with the hardware and software capabilities to be evaluated. It is expected that the TTRF will not be always fully loaded in performing technology transfer research activities. For this reason, it will be used as a test bed to check out new software or new software releases for the TAS. These final tests will be accomplished in the TTRF without adversely effecting the operational use of the COINS-II network.

The TAS in the TTRF will also function as the system to support the training of new COINS users in how to access the COINS network and the rich assortment of resources provided by the COINS host computers.

IV. FACTORS BEARING ON THE PLAN

A. Facts

1. The COINS PMO has agreed to use the TTRF to construct a test bed to evaluate capabilities being developed under the DARPA Man-Machine Relationship Program.

This is a long-term program that will provide new hardware and software and iterative evaluation-improvement cycles. The first version of the electronic desk was delivered to the COINS PMO for evaluation in June 1980.

2. The second version of ADAPT (ADAPT II) was funded by the COINS PMO. ADAPT II must be evaluated in a realistic environment before making it available for operational use. ADAPT II will be delivered in October of 1980.

B. Assumptions

1. COINS will be required to provide information handling services other than query-response.

If this assumption is false, the network development activities will be much diminished, and the TTRF will be difficult to justify.

2. Remote access to the TTRF will be available using standard COINS terminals and other nonstandard equipment for

the purpose of engaging in technology transfer research activities from remote sites; e.g., the intelligence schools and Washington, D.C. area subscriber agencies.

If remote access is not available, then training activities must be treated differently than planned. Also, the approach to capability evaluation of involving users at their home stations will not be possible nor will contractor and COINS PMO personnel have the option of developing or presenting realistic demonstrations of capabilities at the intelligence schools or other sites.

C. Issues

1. Access to computers other than the TTRF DEC PDP-11/70 has not been provided nor are there plans to do so. If arrangements can be made to access computers on the COINS network and other networks (e.g., ARPANET) to evaluate capabilities available on those computers, the technology transfer research activities would be much enhanced. The use of these computers in the entire capability evaluation process would be ideal. However, many technical and organizational problems inhibit or preclude this ideal solution. On the other end of the spectrum, a minimal use of these other computers is to do the preliminary evaluation to determine if additional resources should be expended to do further evaluations. A resolution of the issue that goes as far beyond the minimal use as practical is preferred.

If the status quo is maintained, the hands-on evaluation work will be limited to capabilities that can be made to function on the DEC PDP-11/70. The cut-off point for determining if a capability has enough promise to warrant its implementation on the TTRF computer will be much higher because the cost of evaluation will be higher. The consequence is that fewer capabilities will be examined because the cost to install them on the TTRF computer for further evaluation cannot be justified.

2. It is presently planned that the TTRF staff initially will be contractor personnel. Most of the technology transfer research activities will require access to the substantive intelligence files. If, however, contractor personnel are restricted from accessing many of the substantive intelligence files as they now are, the staff will have to be drawn from in-house resources.

V. APPROACH

The approach to satisfying the long-term objectives of the COINS Network Development is to find cost-effective ways to meet the quantitative and qualitative needs of the COINS user and server communities.

The first step in satisfying a requirement is for the COINS PMO to decide if it can be satisfied by using or modifying a resource available within COINS. Only those requirements that require the

introduction of a resource new to COINS, or that require an existing resource to be significantly changed will be considered Network Developments.

If a resource new to COINS is required, existing or developing resources external to COINS will be evaluated to determine if they can be adopted or adapted to satisfy the requirement. New development will be considered only when it is the most cost-effective way to satisfy the requirements. New developments, once they are tested and ready for evaluation, will be treated in a fashion similar to existing resources that are being considered for transfer to COINS. Step a., in the following general procedure does not apply to new developments.

A. General Procedure

Evaluation of new resources will be conducted by a "technology transfer manager" and his staff within the COINS PMO with assistance from the COINS user community. Once a resource has been designated for evaluation, the following general steps will be taken:

- a. The resource will be installed for preliminary evaluation.
- b. For promising resources, demonstrations to show how the capability may be used in an operational environment will be developed. The demonstrations will use as realistic applications as are practical for a training environment.

- c. Potential users of the resource who are to participate in the evaluations will be shown demonstrations and trained in using the new resource.
- d. A period of supervised use will be provided for the participants.
- e. Access to the capability will be provided to selected users at their home stations, when this is practical, for their use and further evaluation in an operational environment.
- f. The evaluation will be concluded with a report prepared for the COINS PMO by the technology transfer manager with major contributions from the users. The report will include a recommendation: to implement, to modify and implement, to select an alternative capability, to continue in an experimental mode, to do some combination of the preceding, or to discard the resource.

B. Network Development

Management of the net development activities will be the responsibility of the COINS PMO with assistance from a coordination group composed of representatives from the intelligence agencies--CIA, DIA, NPIC, and NSA--and from the State Department and Department of Energy.

The COINS PMO will identify resources for evaluation. To support the evaluation of resources, the COINS PMO will be responsible for:

- a. Developing evaluation plans.
- b. Identifying any additional hardware and software needed for the evaluation.
- c. Acquiring any additional hardware and software.
- d. Coordinating the installation of any additional hardware and software with participating organizations when required.
- e. Developing needed software when development is the most reasonable way to acquire the resource.
- f. Coordinating the evaluation plans with the coordination group.
- g. Developing realistic demonstrations of the capabilities to be evaluated.
- h. Training the resource user who are to participate in the evaluation.
- i. Conducting the evaluations.
- j. Preparing the evaluation reports.
- k. Coordinating the evaluation reports with the coordination group.
- l. Allocating capacity for use by individual users to develop, test and evaluate resources to address their substantive problems.

The coordination group will be responsible for;

- a. Reviewing the resources identified by the COINS PMO for evaluation, identifying additional resources to be evaluated, and prioritizing the resources to be evaluated.
- b. Identifying the substantive intelligence problems that can use the resources to be evaluated and selecting one or more problems for use in the evaluation.
- c. Identifying personnel within each agency who will participate in the evaluations.
- d. Reviewing the evaluation plans and schedules prepared by the COINS PMO.
- e. Reviewing the progress of the evaluations.
- f. Coordinating with the COINS PMO to address any interagency problems that may hamper the evaluations.
- g. Reviewing the evaluation reports prepared for the COINS PMO.
- h. Coordinating implementation actions when it is decided that a capability should be implemented.

VI. STATUS AND PLANS

The near-term plans call for the evaluation of ADAPT-II from October 1980 through June of 1981. The USIS evaluation will start in October of 1980 and run through September of 1981. The first phase

of the Man-Machine Relationship Program (MMRP) will start in FY81. The MMRP evaluation will continue on an as-required basis for several years as additional capabilities are developed. Also the TTRF will be used as the test bed to test and evaluate TCP4/IP and the Kernelized Secure Operating System (KSOS) in conjunction with COINS Access Systems. TCP4/IP and KSOS testing will be accomplished during FY81 and FY82. The initial phase of the prototype BLACKER system test and evaluation will start in early FY81.

During the mid-term (FY83 - FY84) application of computer-aided instruction (CAI) techniques to COINS training will be evaluated in the TTRF. This evaluation will be part of the User Support Information System (USIS). The evaluation of the standard secure network front-end (SNFE) will also involve the TTRF during the mid-term.

The evaluations of RITA, NED, and the graphics package applications to intelligence problems will start in FY83. It is possible, however, that other COINS-PMO development efforts may find use for one or more of these resources prior to FY 83. The Network Usage Information System is a strong possibility for the graphics package and NED provides an easy-to-learn and easy-to-use editor for capturing and maintaining on-line user guides in support of the User Support Information System.

A DEC PDP-11/70 will be delivered in December 1980 for the Technology Transfer Research Facility. The TTRF PDP-11/70 will house the prototype USIS and may be used for the KSOS and TCP4/IP evaluations, although the KSOS and TCP4/IP evaluation will initially

use the Network Service Host in the test bed. In FY83 USIS will be placed on a dedicated computer; freeing the TTRF PDP-11/70 of that work load. At that time the TTRF PDP-11/70 will be installed at one of the intelligence schools with a complement of terminals to support development and training and evaluation. Remote terminals will be installed at the other schools to support training and for evaluating new tools and techniques in a psuedo-operational environment.

The BLACKER hardware and software was delivered in April 1980 and evaluations with NPIC/NDS should start by the end of FY80 and with NSA/SOLIS in FY81. BLACKER will go through a multiphase test and evaluation program through FY84. See Annex D, COINS Network Security for more detail.

VII. RESOURCES AND SCHEDULES

The following tables show the funds budgeted, programmed and planned to perform the network development activities that are not included in the other annexes to the long range plan. Annex B, COINS Network Resources presents the resources and schedules for ADAPT, USIS and the TCP4/IP evaluations. Annex D, COINS Network Security, presents the resources and schedules for the BLACKER, Kernalized Secure Operating System (KSOS) and the Secure Network Front End (SNFE) evaluation.

FY 79 funds were used to procure the DEC PDP-11/70 TTRF computer, and therefore are not reflected on the following table.

The funds shown on the following tables are for evaluating existing capabilities or capabilities being developed with project funds external to COINS.

A. Man-Machine Relationship Program (MMRP)

	FY 80	81	82	83	84	85	86
O&M PROCUREMENT RDT		40	50	100	100	100	100
TOTAL		40	50	100	100	100	100
1000 of Dollars							

B. RITA

	FY 80	81	82	83	84	85	86
O&M PROCUREMENT RDT&E				75			
TOTAL				75			
1000 of Dollars							

C. TEXT EDITING/WORD PROCESSING (NED)

	FY 80	81	82	83	84	85	86
O&M PROCUREMENT RDT&E				80	80	80	80
TOTAL				80	80	80	80
1000 of Dollars							

D. GRAPHICS

	FY 80	81	82	83	84	85	86
O&M							
PROCUREMENT							
RDT&E				75	75	75	75
TOTAL				75	75	75	75
1000 of Dollars							

E. ADAPT, MMRP AND RITA INTEGRATION

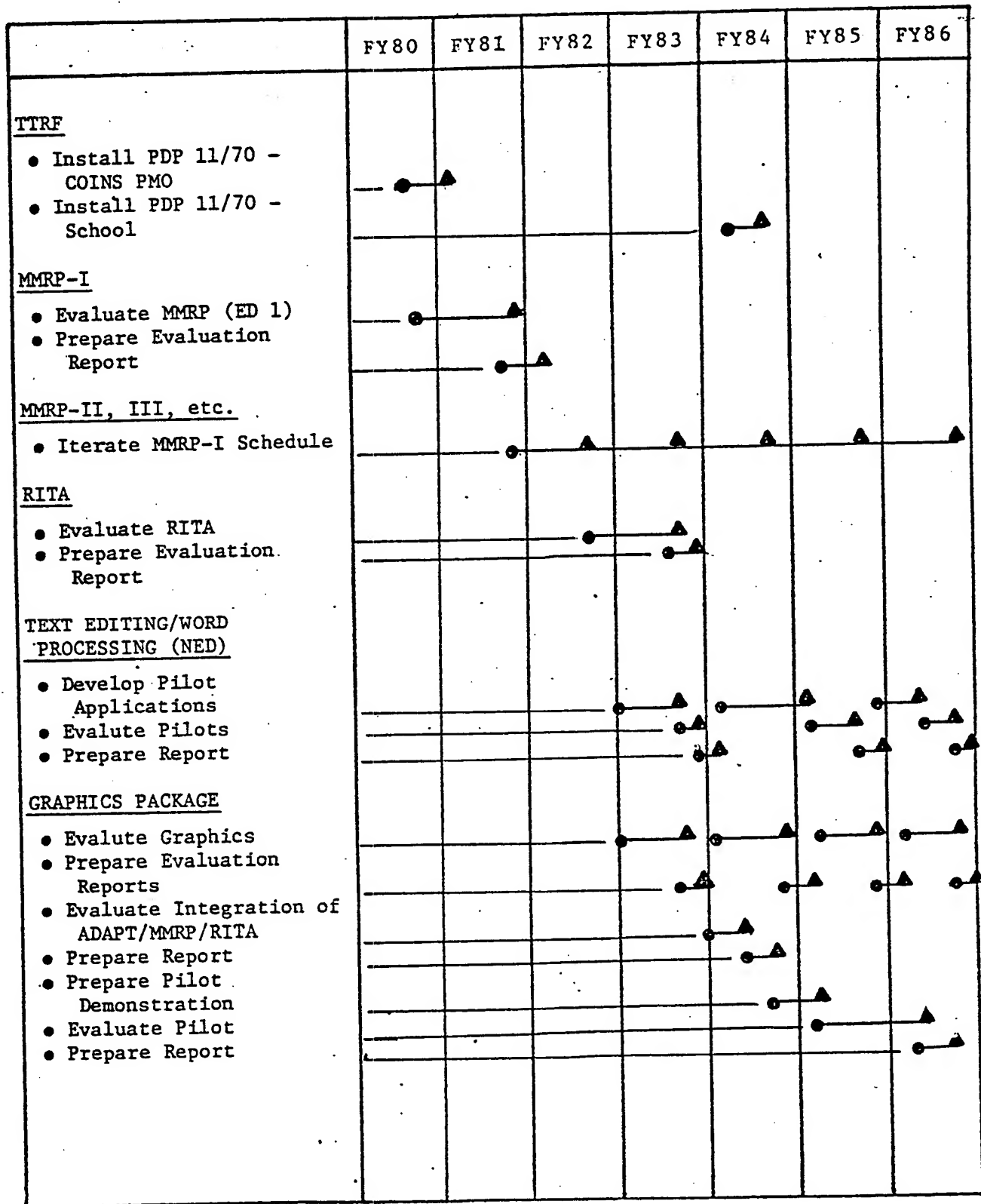
	FY 80	81	82	83	84	85	86
O&M							
PROCUREMENT							
RDT&E					175	175	175
TOTAL					175	175	175
1000 of Dollars							

The RDT&E funds in FY84 are to evaluate the integration RITA, ADAPT and the extant MMRP capabilities into an analyst work station. The FY85 funds are to develop a demonstration of how the integrated capabilities can be used on a realistic analyst problem.

F. TOTAL NETWORK DEVELOPMENT

	FY80	81	82	83	84	85	86
O&M		—	—	—	—	—	—
PROCUREMENT		—	—	—	—	—	—
RDT&E		40	50	330	430	430	430
TOTAL		40	50	330	430	430	430
1000 of Dollars							

SCHEDULE



APPENDIX

CAPABILITIES FOR EVALUATION

The capabilities to be considered for evaluation in the network development activities are MMRP, RITA, the Text Editor (NED), and a Graphics Package. A separate plan will be developed to cover the evaluation of each capability.

The following paragraphs present brief descriptions of these capabilities, and some general applications for RITA, NED and the Graphics Package. These kinds of general applications will be used in addressing realistic problems in the evaluations.

Man Machine Relationship Program (MMRP)

Description:

The MMRP is a research and development project being funded by DARPA. It includes hardware and software development. The main thrust of the project is to determine the characteristics of a work station at various levels of endeavor; i.e., from analyst level through the policy making levels of government. The hardware and software are presently in their embryonic state. It is expected that many incremental improvements will be made over the next several years.

RITA

Description:

Rule-directed Interactive Transaction Agent - is a system designed for use by persons who are not computer sophisticates to develop agents (computer programs) to perform tasks in an automated fashion. It is under development by Rand and is experimentally operational.

Applications:

- Preparing and maintaining human-machine interfaces tailored to individual analysts.
- Preparing and maintaining programs to perform simple repetitive analyst's tasks,
e.g., monitoring data for abnormal or out-of-bounds activities.
- Updating stored queries to reflect changes in such things as date of coverage, area of coverage and VIPs of interest.
- Invoking queries based on the determination that an event occurred.

Status:

RITA is experimentally operational on the Network Service Host and will be operational on the TTRF in September 1980.

NED

Description:

A CRT text editor developed by Bolt Beranek and Newman, Incorporated under contract to the Rand Corporation. It is used with a CRT terminal to prepare and modify documents, letters, messages, and computer programs.

Applications:

- Preparing periodic and ad hoc reports.
- Editing personal files, e.g., query responses.
- Incorporating query responses into reports.

- Preparing queries for submission.
- Combining query responses from different files into a uniform format.
- Introducing or suggesting changes on collaborative reports.
- Preparing messages for electronic or hard copy delivery.
- Preparing and maintaining briefings in a current fashion.
- Preparing and maintaining computer programs including RITA programs.

Status:

NED is currently operating on the NSH with both Ann Arbor 4080D CRT terminal and the Teletype Model 40 CRT terminal.

NED will be made operational on the TTRF after it is installed.

GRAPHICS PACKAGE

Description:

The set of PLOT 10 programs and a Hewlett Packard HP 2648 graphics terminal to provide a general purpose graphics capability for evaluation.

Applications:

- Plotting aircraft and ship movements on map backgrounds.
- Providing graphical representations of tabular data such as flight activity,
 - Ships operation out of area,
 - Long term trends in force changes.
- Preparing graphics for briefings.

Status:

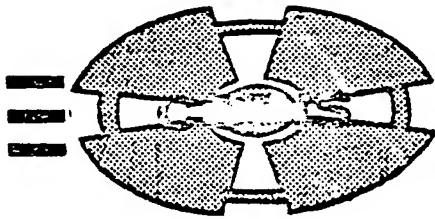
PLOT 10 is operational on the Network Service Host. It will be made operational on the TTRF after it is installed.

Community On-Line Intelligence System

Project Management Office

National Security Agency

Fort George G. Meade, Maryland, 20755



COINS NETWORK SECURITY

ANNEX D

TO

COINS TECHNICAL SUPPORT PLAN

Prepared by
James P. Anderson Co.
7 August 1980

FORWARD

This paper provides the Technical Support Plan for the COINS Network Security. Readers who desire or need more information about the COINS PMO plans for network security are referred to the COINS Network Security Development Plan.

TABLE OF CONTENTS

	<u>Page</u>
FORWARD	iii
I. DESCRIPTION	D-1
A. Overview of CAS Security Architecture	D-3
1. Structured Network Identifiers (SNI)	D-4
2. Access Authorization	D-5
3. Server-Host Authorization	D-6
4. Decentralized Security Management	D-6
II. LONG-RANGE OBJECTIVES	D-8
III. JUSTIFICATION	D-9
IV. FACTORS BEARING ON THE PLAN	D-10
A. Facts	D-10
B. Assumptions	D-11
1. General Assumptions	D-11
2. Technical Security Assumptions	D-12
C. Issues	D-13
V. APPROACH	D-17
A. KSOS/TCP4 Applied to CAS/NAS	D-19
B. Multi-Jurisdictional Security Protocols (Need-to-Know Controls)	D-19
1. Approach	D-19
C. BLACKER	D-21
D. BLACKER Applications	D-22
E. Secure Network Front-End	D-23
F. Improved User Identification and Authentication Techniques	D-24
G. Software Encryption in TAS/CAS	D-25
1. Encrypted Personal Files	D-25
2. Encrypted Passwords	D-25
3. Surrogate Log-On Protection	D-25

TABLE OF CONTENTS (Concluded)

	<u>Page</u>
H. File Output Labeling	D-26
I. Network Access Control to COINS	D-27
J. Network Security Officer Support	D-28
K. Network Security Architecture	D-29
VI. STATUS AND PLANS	D-30
A. KSOS/TCP4	D-30
B. Multi-Jurisdictional Security Protocols	D-30
C. BLACKER	D-30
D. BLACKER Applications	D-30
E. Secure Network Front-End	D-31
F. User Identification and Authentication Techniques	D-31
G. Software Encryption in TAS/CAS	D-31
H. File Output Labeling	D-32
I. Network Access Control to COINS	D-32
J. NSO Support	D-32
K. Network Security Architecture	D-33
VII. RESOURCES AND SCHEDULE	D-33
A. KSOS/TCP4	D-33
B. Multi-Jurisdictional Security Protocols	D-34
C. BLACKER	D-34
D. BLACKER Applications	D-35
E. Secure Network Front-End	D-35
F. Improved User Identification and Authentication	D-36
G. Software Encryption	D-37
H. File Output Labeling	D-37
I. Network Access Control to COINS	D-38
J. NSO Support	D-38
K. Security Architecture	D-39
SUMMARY OF COSTS	D-39
SCHEDULE	D-40
REFERENCES	D-41

I. DESCRIPTION

The COINS security plan is an integration of a number of projects designed to provide maximum protection to Sensitive Compartmented Information (SCI) and other classified material handled in the network.

The present state of COINS security is summarized below:

- a. The COINS network operates in a System High mode of TOP SECRET SI/TK. All COINS users are cleared TOP SECRET SI/TK.
- b. All COINS users are transaction system users. There is no user programming accessible through COINS on any server-host in the network.*
- c. Batch operations follow TMA-3⁽¹⁾ security rules.
- d. All COINS computer and terminal sites are cleared for TOP SECRET SI/TK operations.
- e. COINS security issues are handled by the COINS Network Security Officer (NSO) who is the chairman of an inter-agency committee known as the COINS Security Panel.
- f. Formal security procedures for the COINS Terminal Access System (TAS) are being developed. These procedures will delineate the security duties and responsibilities of the TASMASTER, administrative users, and individual end-users.

*Since COINS exercises NO control over server-hosts, it is possible that a participating agency will provide programming access for its own users on the server-host upon which a COINS data base is homed. However, such programming access IS NOT available from the COINS network.

- g. The original COINS Security Panel (CSP) charter is being updated and reissued. The new charter will identify CSP members as the ISSOs for the various participating agencies. The chairman of the panel will be the COINS Network Security Officer. The CSP will continue to advise the COINS Project Manager regarding security policy, implementation of security measures, and security research needs of the network.
- h. COINS has no independent security authority. It has no authority to impose security requirements on or police the enforcement of existing security policy by either user or contributing agencies. As a designated community-wide service, COINS derives its security requirements from DCID's 1/16, 1/7, and 1/14;^(2, 3, 4) Executive Order 12036 (for Privacy)⁽⁵⁾; and USCSB 4-11 for policy on compromising emanations.⁽⁶⁾ COINS does have both the authority and independent jurisdiction over the security of the COINS Network (i.e., the secure subnet and the interface layer of TASs and NAS).
- i. Each participating agency is responsible for insuring the safety of its segment of the system, including procedures to protect access to files by authorized terminals or personnel and providing for proper security labels on system outputs. Each agency has also appointed a representative to the COINS Security Panel.

j. Although extensive security controls have been designed into the COINS Access Systems (CAS) (see below), only about 10% of the COINS user population is currently homed on a CAS.

k. Just as the CAS was seen to provide a standard and coherent interface to users, it also provides substantial security functionality as well.

A substantial part of the technical COINS security development to date has been focused in the COINS Terminal Access System (TAS) (7, 8, 9). Since its development, the TAS has evolved into a generalized network interface and access system (CAS) which will perform the functions of a network front-end and internet gateway as well.

Because of the central role the CAS plays in the overall approach to providing COINS security, a review of the principal security features of the CAS is presented as a base from which additional developments will be made.

A. Overview of CAS Security Architecture

The CAS architecture is responsive to the diverse and dynamic nature of the COINS network. It provides the user a coherent interface to server-host computers of different manufacturer and to data base applications of widely varying design. It was conceived as a means of insulating its users from much of the differences that exist in the different server-host machines and the data base query languages.

The CAS security architecture has been designed to provide maximum protection to the sensitive data in the network while keeping the end-user's interface as simple as possible.

In addition, the CAS security architecture has addressed the problem of security administration. It provides the user organizations with considerable flexibility in how security is managed. It also allows a single CAS to support more than one organization, each of which can exercise full control over its own security management yet be isolated from and non-interfering with other co-resident user organizations.

The principal features of the CAS security architecture are:

- a. Structured Network Identifiers
- b. User Access Authorization
- c. Server-Host Access Authorization
- d. Decentralized Security Management

These topics are discussed in more detail below:

1. Structured Network Identifiers (SNI)

All CAS users are uniquely identified with an eight-character identifier of the form:

TAAGGUUU

where:

T = is the user's home CAS

AA = is a designator representing the user's agency

GG = is a group within an agency

UUU = is the user within the grouping. (A number in the range 000-999)

The structured identifier uniquely identifies all network users entering through CAS and permits both activity and security logging of an individual's network activity. A user requires an SNI and a password to log on to CAS.

2. Access Authorization

Each user known to a CAS (i.e., who has an SNI) has an access authorization record in the User-Host Access Authorization (AA) File (UH/AAF).

In addition, the record contains a list of the COINS application (e.g., RYETIP, SOLIS, DIAOLS, ADCOM, etc.) and, for those applications involving multiple files, a list of files authorized to the user by the user's home organization.

The user's access authorization record also contains interactive systems log-on information (an identifier and password) in the form required by the particular interactive system. This information is used to perform a user-invisible log-on to the server-host supporting an interactive application. This "surrogate log-on" service of CAS insulates COINS end-users from the considerable variability in log-on protocols that exist among the computer systems of COINS.

Application and file access controls are applied to terminals as well. Each terminal connected to CAS is logically identified by CAS and is represented by an AA record defining which applications and files within the applications may be accessed by the terminal.

A "session security level" is logically established at log-on based on the user's authorization and his terminal's authorizations. This (conceptual) level controls what data may be accessed in a session.

The user and terminal AA files are used by CAS to implement the major functions of TMA-3:

- Control of user access to a data base
- Verification that a user/terminal is cleared to receive a particular batch response

3. Server-Host Access Authorization

When CAS was upgraded to include server-host functions in 1978, the access authorization function was expanded to include application access authorization data.

4. Decentralized Security Management

The CAS security management design was influenced by the following major considerations:

- Each using agency would be responsible for managing the security information and access authorizations of its own users and applications (where appropriate).
- A large using agency may wish to delegate some of the security management to functional organizations within the agency.
- A single CAS may be shared by two or more independent agencies.

To meet these somewhat diverse requirements, the CAS security architecture includes three kinds of users:

TASMASTER - a single user who "owns" the CAS and who directly or indirectly (see Administrative User) creates all other users.

Administrative User - a user who has the delegated authority to create and administer a specified set of ordinary users.

Ordinary Users - users authorized to use CAS and the COINS network.

An administrative user can add, modify, or delete users within the group that can be "named" with a single "SNI-prefix". That is, the up to 1,000 users who have the same TAAG (CAS, Agency, Group within the Agency) prefix in their SNI.

Administrative users cannot affect any records other than those bearing the same SNI-prefix.

The TASMASTER establishes the basic access authorizations for administrative users. The administrative user can further subdivide his access authorizations among users within his domain. He cannot give any user more privileges than he has himself. It is not necessary to give an administrative user all CAS or network privileges.

II. LONG-RANGE OBJECTIVES

The objectives listed here are the security-related objectives for COINS itself. The objectives provide the targets to shoot for and an independent basis of evaluating how well COINS meets the objectives. Some objectives require management/organizational initiatives, while others are satisfied by technical research or development activities.

The following are the security objectives for COINS:

- a. Insure compliance with DCID 1/16 and 1/7.^(2,3) Provide the standardized security markings of DCID 1/7⁽³⁾ within the COINS network.
- b. To evolve with the use of the network, supporting the security interests of users and servers alike.
- c. Demonstrate the capability to perform multi-level secure handling and processing of information in the network.
- d. To provide better access to COINS, improve NTK controls, provide closed communities of interest (COIs), and misroute protection in COINS by continuing to develop and refine the ongoing BLACKER project.
- e. Improve the technical foundation for COINS security and provide support for some user programming in the network by applying KSOS to one or more network service hosts.
- f. To support expanded usage of COINS for:
 - Data base applications
 - Development of special uses and other kinds of transaction systems

- g. To offer cost-effective solutions to security problems arising from internetworking.
- h. Provide the ability for the network to handle multi-jurisdictional security protocols for NTK.
- i. Integrate the capabilities of the UNIX-based CAS/NAS with the BLACKER and KSOS to produce a secure NFE suitable for use in COINS and other integrated service networks.

III. JUSTIFICATION

Aside from the obvious justification for providing security of sensitive information, the underlying reason for the elements of the COINS Security program is to improve the usability of the network. The usability of the network is closely tied to the ability of the network to provide security and need-to-know protection for the information resources being handled on the network. Since the CASs have a role in providing local user services, they ought to be able to do so securely.

At present, much of the CASs' security is derived from the limited user functionality they present. As we move through the 1980's, limitations on user functionality will severely hurt the network's development. Thus, both the KSOS/TCP4 and BLACKER programs are meant to provide a better technological foundation for continued network growth.

As more COINS Access Systems are installed as gateways, front-end and terminal access systems, server-hosts can be relieved of a substantial administrative burden or keeping track of all of the users,

precluding some users from accessing proprietary information and the like. At this moment, the full burden of protecting a server's assets falls on the server-host's agency. In the very near future, to the extent and scope desired by the server agency, that burden can be shifted onto a CAS front-ending the server. The CAS will be able to enforce the security requirements and whatever need-to-know or proprietary access policy is desired by a server-host/application on users accessing the host from the network.

Finally, a number of tasks described in this plan are included to improve the security management and security administration of the network.

IV. FACTORS BEARING ON THE PLAN

A. Facts

1. COINS is currently operating at the TOP SECRET SI/TK level, providing support to approximately 2,400 users in 40 different organizations. The single security level (systems high) mode of operation restricts the use of the network to only those users with TS-SI/TK access authorizations.
2. The UNIX-based CAS has built-in access and distribution security and need-to-know controls. This capability provides an important foundation upon which additional COINS network security can be built.

3. ASD(C³I) has tasked COINS PMO to work with DCA to develop a standard secure network front-end (SNFE). A standard SNFE will reduce the costs of providing secure networks, not only in COINS, but in other user communities.

B. Assumptions

1. General Assumptions

a. COINS will continue to operate in the Washington, DC, area through FY 1986 and will be expanded to:

- Provide service to intelligence analysts in all appropriate agencies
- Provide different types of information handling services, other than query-response (e.g., teleconferencing, text editing, specialized planning systems, and the like) to intelligence community end-users
- Incorporate additional host processors and other applications

Even if the assumption about COINS growth proves to be incorrect, most of the security elements outlined in this plan are still required. About the only part of the plan that might not be required under the assumption of no further growth is the part containing the elements leading to multi-level secure operations.

b. COINS will have gateways to other networks. If this does not come to pass, then the segments of the security plan designed to cope with supporting users on other networks will not be required.

c. COINS will come under increasing pressure to provide multi-level secure operation, not only to gain access at the appropriate level to data classified only SECRET or CONFIDENTIAL, but to support access to more and different kinds of SCI. In addition, COINS will have to show that it can control access, NTK and delivery of data to individual users and or terminals by name in order to meet the security requirements of the APEX system.

d. There will be no relaxation of security constraints on COINS or other community systems in the next five years. Some additional need-to-know approvals or originator-controlled data requirements may be added during this time period.

2. Technical Security Assumptions

a. The BLACKER prototype system will be sufficiently successful that it will be possible to incorporate BLACKER concepts and equipment in network security plans not later than FY 1985.

b. The UNIX KSOS will be certified in 1980, such that the proposed TCP4/KSOS test bed can be established no later than the end of FY 1981. This assumption affects not only the objective of developing a multi-level secure network of COINS, but its failure or delay will affect the extension of BLACKER to other network elements.

c. The design and implementation of the CAS will continue to be improved to permit responsive simultaneous connection of at least 64 subscribers, under KSOS implementation. This assumption is an implied performance objective for KSOS. While it is not anticipated that the initial installation of KSOS will meet this objective, if it appears that the objective can never be met, the entire concept of a multi-level secure COINS network will require serious reexamination.

d. The results of the DARPA BCR project will continue to be available to COINS, particularly the work regarding multi-jurisdictional security administration. Since in some regards the BCR project is a "shadow" BLACKER, it is important to COINS as a backup to the BLACKER project and as a possible means of providing the NTK and COI protection in the event of a serious failure of BLACKER.

C. Issues

1. There is a potential for conflict regarding how to apply particular technological developments to achieve a desired capability for COINS. The potential arises from how one looks at the network--as a set of logical circuits (analogous to wire) or as an integrated service to a community of users. These views lead to different interpretations of what is important.

Failure to recognize this issue can lead to dilution of COINS to a mere wire-works. While it is technologically possible to effect such connection(s), the question is whether or not the purpose and function of COINS is served by doing so.

If the issue is resolved in favor of the logical circuit view of the network, then much of the network security plan, and other "user services" designed to be integrated in the access ring is unnecessary. It will also result in a network where the burden of using the network will be substantial, and on the shoulders of the user alone.

If the issue is resolved in favor of the value-added view of the network, then the BLACKER technology will have to be adapted (in some ways, substantially) in order to serve COINS needs. To a much lesser extent, there are similar trade-offs applicable to the KSOS if it is applied throughout the network.

The issue requires a careful understanding of the alternatives, not only in the security sphere, but in the COINS PMO provided services as well. It does not appear that both views can coexist, therefore, a choice will have to be made as to which view will guide COINS development over the next decade.

2. Server-hosts supporting applications contributed to COINS or providing terminal support to users in their agencies may operate under different security regulations than COINS (e.g., a DoD regulation implementing the Executive Order ⁽⁵⁾—and the DCID 1/16 ⁽²⁾ and DCID 1/7 ⁽³⁾. Regardless, COINS cannot enforce Department/Agency regulations beyond those specified in DCID 1/16 ⁽²⁾ and DCID 1/7 ⁽³⁾.

3. Overall security in the current network will be considerably improved if:

- No user programming is permitted on any COINS server-host.
- All "local" users of any COINS server-host were homed on a CAS.
- All COINS users were homed on a CAS.

Even if everyone agreed to the correctness of these points, there is no way to effect the changes required since COINS does not own or control the essential assets (server-hosts, applications, etc.). At present, all that can be done is to attempt to persuade the various entities to move to these positions. The development and integration of multi-level secure processors will remove the need for such restrictive measures.

4. The internetworking of COINS with other networks (PLATFORM, IDHSC, etc.) creates multi-level networks (networks of at least System High level in DCID 1/16 ⁽²⁾ terms).

The DCID 1/16⁽²⁾ "Compartmented Mode" as defined provides less control than System High (as defined) unless the user's functionality is restricted in some way not specified in the DCID.

V. APPROACH

The security plan outlined here is directed to developing and applying various technical measures to COINS to achieve some or all of the objectives outlined in Section II. In addition, the plan provides for the administration of COINS security through the COINS Network Security Officer. A number of items are for support of his effort(s).

The plan presents short-term (one to three years into the future) and longer-term (three of five years and beyond) elements. To some extent, the plan is paced by the short-term objectives. Further, some of the longer-term objectives will be mediated by how the network evolves from its present form. The contribution of the various elements of the plan to the objectives outlined in Section I are illustrated in Figure 1.

The principal approach to providing COINS security is to require that all users of COINS be registered (known) on some CAS (a TAS, HAS, or NAS) depending on where the end-user is located. With all network users registered and known on some network asset, it is then possible to enforce access controls at the various COINS Access Systems. This, coupled with anticipated developments in KSOS and BLACKER to protect the access control mechanisms themselves, will provide flexible and efficient network security.

<div>Program Element</div> <div>Objective</div>	KSOS/TCP4	NTK Controls	BLACKER	BLACKER Applications	SNFE	ID & Authentication	Software Encryption	Output Labeling	Network Access Controls	NSO Support	Security Architecture
1. Comply with DCID 1/7, 1/16								X			X
2. Support network evolution	X	X		X		X	X	X	X	X	X
3. Demonstrate multi-level capability	X		X								
4. Improve NTK, COI controls	X	X	X	X			X	X			
5. Improve technical foundation of COINS security	X			X						X	
6. Expand usage of COINS	X	X	X	X		X	X	X	X		
7. Provide internetworking									X		
8. Handle multi-jurisdictional controls											X
9. Obtain a secure network front-end for integrated networks			X		X						

FIGURE 1

Contribution of Plan Elements to COINS Network Objectives

A. KSOS/TCP4 Applied to CAS/NAS

Problems to be solved:

- a. Improved technical foundation for COINS security
- b. Support for TAS user programming
- c. Increased confidence in multi-jurisdictional security controls

It is planned to implement the CAS functions under a KSOS system operating in the computer, supporting the TTRF. This development will also address the TCP4 implementation, either directly or in the "torque-converter" mode of operation.

B. Multi-Jurisdictional Security Protocols (Need-to-Know Controls)

Problems to be solved:

- a. Need-to-know (disjoint compartments)
- b. Handling the large number of users (1,000-5,000) anticipated in the next two to four years

1. Approach

As soon as a sufficient number of CASs are deployed, each participating agency will be required to register all of their own COINS users in a CAS system. The registration will be as though the user is a CAS subscriber and will include a description of all COINS accessible services authorized for that user by the user's home agency. The registration will be made by (personnel under the supervision of) an identified Security Officer of the participating agency (that is, the agency's ISSO).

Agencies participating in COINS with (one or more) server-host system that also home some or all of the user population of that agency will register their users of COINS on the HAS used to front-end the host(s). TAS users are registered on their TAS. Other network COINS users are registered on the COINS part of NAS.

All registered COINS users will be known by an SNI. SNI groups will be assigned to each participating agency and managed by that agency on an on-site CAS or a CAS assigned by the COINS PMO.

The ISSO of the CAS in a sponsoring agency is responsible for establishing and maintaining the Server-Host/Access Authorization File (SH/AAF) in the CAS which identifies which using organizations in the COINS network or other networks can have access to specific files or services available in the CAS, the host, or network behind the CAS.

The SH/AAF will be used to build and maintain the NSO's Master Authorization File (MAAF) in the Master TAS in the COINS PMO. The MAAF will be built and maintained on-line at the Master TAS either automatically or upon command of the NSO by retrieving a current copy of the SH/AAF from each CAS including the Master TAS. After the SH/AAF file has been received from each CAS, the MAAF is sorted by using organization and used by the NSO to establish the SH/AAF for each CAS.

C. BLACKER

Problems to be solved:

- a. Closed Communities of Interest (COIs) in COINS.
- b. Misroute
- c. Malicious system software (not necessarily in COINS).

The BLACKER development is directed to providing a unique end-to-end encryption between an individual user and a process on a distant host.

The initial BLACKER system, installed in the COINS-II network in April, 1980, is a prototype system. The two agencies participating in this program are NSA and NPIC. This involves the installation of a special front-end device and the installation of a specially-designed BLACKER Terminal Access System.

1. Users operating from a remote terminal on the BLACKER terminal access system will be authenticated by a COMSEC system, and if properly authenticated, the user will be connected to the appropriate host in the network via a unique one-time secure communication path. Eventually, a badge reader must be associated with each terminal for user identification. The badge which is used for controlling access to a building and compartments within a building will be used to control access to COINS-II via a remote terminal.

2. If a host misdirects an answer or response to a terminal, it cannot be read by the users at that terminal because they will not hold the key.
3. For routine purposes, the headings will be in the clear within a communications processor or TAS. The text will be encrypted and can be read only by the appropriate user/terminal or system. The headers will be encrypted between communications systems; i.e., IMPS.

D. BLACKER Applications

System studies are required to find the best approach to altering the BLACKER prototype or using the basic BLACKER cryptographic equipment to make it compatible with the COINS network philosophy and ultimately to integrate it into an SNFE (see E., below). Integration of BLACKER technology with the SNFE is treated under that program element.

The principal potential application of BLACKER in COINS is in protecting the terminal to CAS link. While there is little or no requirement for such protection within the COINS network, there is a substantial requirement for terminal-to-access ring protection, particularly if COINS subscribers are going to be homed on networks about which little if anything is known. Thus, use of BLACKER to encrypt from a terminal (user) to the user's home CAS provides considerable improvement in security for terminals homed on other networks. BLACKER is also expected to offer a more economical host-to-host secure connection than that currently provided by the PLIs being used to link CASs through ARPANET.

E. Secure Network Front-End

There is a growing body of technology available to provide secure computing of various kinds; this includes the BLACKER work and KSOS. In COINS, a generalized server-host front-end has been developed around the UNIX-based TAS. This is called HAS. HAS houses all of the current TAS functionality and a host-specific interface. This provides considerable flexibility in how the HAS can be employed; the range is from a simple network interface (repository of network protocols) to a system that interfaces both the server-host and local terminals to the network and to each other. In both modes, the HAS can (and does) perform access authorization functions and in general act as a coarse security filter for its server-host.*

In view of the broad range of functions a HAS could perform, the problem of "merging features of BLACKER, KSOS, and HAS into a single SNFE" is substantial.

To some extent, the plan to put TAS under KSOS will provide an excellent start for an SNFE. It will provide per-process isolation and demonstrated secure multi-level partitions.

*It is important to note that the reason HAS or any other similar system cannot perform a full security filter function is because the detailed security decisions (e.g., access limited to a single file or limited to a specific set of tags) are bound into the server-host application (e.g., SOLIS) in a way that cannot be broken out to be resolved at the time access is attempted. In a similar way, some security determination can only be done during the execution of a particular query. As a consequence, the HAS or any front-end can only screen out organizations/individuals who are not authorized any access to the application.

The principal problem to be solved in an SNFE design is how to partition the design and integrate the BLACKER and KSOS technologies into a system that can be used as an unintelligent SNFE (i.e., one with network protocols only) but which could become the base of a more fully functional system such as a CAS by merely adding the additional software modules.

F. Improved User Identification and Authentication Techniques

Problems to be solved:

- a. Reduce the burden of users having to learn different identification and authentication protocols for systems and networks in the community.

While COINS has eliminated the problem of having to learn or know five to eight (or more) different log on and authentication protocols within the COINS network, the COINS approach does not help analysts who must use other networks and systems besides COINS, particularly if they do not access the systems through COINS.

While there is not at this time a satisfactory universal unique personal identification method or scheme, the possible use of magnetic stripe badge readers (with agency identification badges), or some similar scheme, will be explored in conjunction with the BLACKER project. A cost-benefit analysis will be made of the schemes tested and will be used to initiate future procurement should the results be favorable.

G. Software Encryption in TAS/CAS

Problems solved:

- a. Provides protection of passwords and personal files from accidental disclosure
- b. Provides privacy of personal files/messages

1. Encrypted Personal Files

Since TAS will continue to operate in a benign environment for the foreseeable future, the encryption of personal files is more to provide user-controlled privacy than for security purposes. As in many aspects of system use, it should be possible to give the encryption capability selectively; i.e., some users can have it as a function, others cannot.

2. Encrypted Passwords

The purpose of encrypted passwords is to prevent compromise of a user's TAS log-on password from disclosure to TAS operations personnel. A traditional method of providing this protection is to store in the user's log-on file a password transformed (encrypted) by a one-way function. Upon log on, the plain text password submitted by the user is subjected to the one-way transformation and the result compared with that stored in the user's record.

3. Surrogate Log-On Protection

The requirement for surrogate log-on protection is similar to that needed for protecting the TAS log-on password. It is desirable to prevent compromise from TAS operations personnel.

Unlike the TAS log-on password, the requirement is not met by a one-way transformation. A major question to be addressed is whether the entire AA File record for an individual is to be protected or whether just the surrogate log-on passwords for SOLIS, IDS, etc., must be protected.

It appears at this juncture that it will only be possible to protect the Access Authorization Files (AAF) from TAS operations personnel if a protected cryptographic facility (e.g., BLACKER key generator or DES) were provided in the TASs and each host (or CAS). To implement a scheme of encrypted files (AAF) while providing essentially the same functionality to the administrative user (to create and maintain individual users) requires a host-to-terminal and host-to-host secure communications capability. The scheme and adaptation of the IBM key management model outlined in IBM Systems Journal, Vol. 17, No. 2 of 1978, would limit the exposure of AAF data in a TAS to the (single) individual who could set a Host Master (cryptographic) Key. This scheme would require both a crypto-facility (essentially a computer-controlled crypto-peripheral) and a KSOS foundation to provide adequate protection from TAS operations personnel.

H. File Output Labeling

Problems solved:

- a. Compliance with DCID 1/7. (3)

At present, the COINS network carries security labels on the responses to batch queries. The security labels are used only to check the authority of the terminal and/or the user to receive the level of material contained in the answer.

DCID 1/7⁽³⁾ requires appropriate security labels to be applied to all classified materials. In order to comply with this requirement, it is necessary to provide security labels on all data bases and files in the COINS network. For those files associated with batch applications, the security labeling is provided by the server-host in compliance with TMA-3. In the case of SOLIS, security labeling is applied on a per-message/record basis. Since SOLIS did not have a batch interface requirement, there was no reason to implement TMA-3. With respect to attempting to implement proper security labeling of output in compliance with DCID 1/7⁽³⁾ for COINS, it is necessary to recognize the fact that TMA-3 is not an integral part of the interactive applications.

I. Network Access Control to COINS

Problems solved:

- a. Increased accessibility of COINS
- b. Reduced costs for connecting subscribers

In general, it is assumed that the gateways will be on the host-to-host form (access layer) as opposed to internet level gateways alone. The host-to-host form is suitable if it is

assumed that there is little or no requirement to provide end-to-end connections between subscribers homed on other networks and a process on the COINS network. The proposals assume that a gateway-half concept⁽⁵⁾ will be used. This form has a natural appeal and addresses the ownership of the gateway and the contained network access control mechanism properly. In addition, as a principle, the notion of each network providing its own access control makes considerable sense.

J. Network Security Officer Support

- a. Provide automated aids for security officer surveillance of network use

Currently, System Security Officers (SSOs), in those installations having them, get abstracts from the computer accounting logs where all major normal and potentially abnormal activity (e.g., unsuccessful log ons) are recorded. The unsuccessful log ons are just about the only major information received from most computers, even though other data may also be available (e.g., unauthorized file access attempts). Aside from the fact that the data recorded is not primarily for security purposes, the primary value of security audit logs currently derived from accounting data is retrospective analysis of attempts at external penetration.

The basic approach to Security Exception Reporting is to establish on a per-user (or per-file, application, or other controlled resource) basis a "profile" that characterizes

"normal" use of the resource. The profile can then be matched against actual use of a resource to determine whether any user activity is "out-of-range" with respect to the profile. Such out-of-range activity can be reported as an exception requiring further investigation, or it can be the basis for detailed analysis of users' actions to determine whether the activity is authorized.

A prototype system exists on a commercial network that could be the basis for a similar system for COINS. Development of such a system will require much of the access ring in place to be effective.

K. Network Security Architecture

Problems solved:

- a. Continued long-range security planning
- b. Identification of network security needs.
- c. Tracking of security developments for application to the COINS network

During the history of COINS, there has been a requirement for a continued, long-term planning and study activity concerned with COINS security issues.

A single, continuing task is involved to continue to survey the security needs of the network and make recommendations for the solution of security problems uncovered.

early investigations will begin in 1981. System studies, integrating the results of the BLACKER evaluation and the requirements for internetworking will identify the best way of using BLACKER in COINS and suggested system alteration for BLACKER.

E. Secure Network Front-End

No work has been initiated on this project.

F. User Identification and Authentication Techniques

The identification of a badge reader system has been made and it is expected that a reader will be acquired by early FY 1981 to integrate with the BLACKER test. The utility of the badge reader as an improvement in user identification and authentication will be evaluated.

G. Software Encryption in TAS/CAS

No work has been done on encrypted personal files to date. The application of the Crypt function of UNIX7 will be evaluated in this role.

No work has been done to implement encrypted passwords in COINS to date. It requires the development of an adequate "one-way" transformation, and its integration in the log-on process. Some work has been done on this process in UNIX⁽¹⁰⁾.

Due to the uncertainties of BLACKER and KSOS deployment in COINS, no work is planned for dealing with surrogate log-on protection at this time.

H. File Output Labeling

In order to determine the most effective, minimum-cost solution to this particular problem, it will be necessary to establish network standards for labeling of output. Standards already exist in TMA-3 but these will have to be updated and possibly modified to accommodate systems that are intrinsically interactive but which may be treated as though they are batch. No work has been done on this task to date.

I. Network Access Control to COINS

At present, a tailored gateway to ARPANET is provided to interface the PACOM TAS. A "one-way" tailored gateway from PLATFORM to COINS is also being developed.

A generalized gateway to COINS is planned using the concept developed by CSC of the gateway-half.⁽¹⁶⁾ The development of the generalized gateway will focus on what kind and how much functionality to put into the gateway (e.g., security functions, register users, etc.).

J. NSO Support

There is no current development to support the NSO. Aspects of operating as the NSO and TASMASTER are being explored as part of a general TAS upgrade effort.

The security surveillance system and monitoring tools will be defined and evaluated starting FY 1982. The entire development should be complete by the end of FY 1984.

K. Network Security Architecture

This function is currently being performed by one of the COINS PMO contractors in association with the NSO. It is planned to continue this function as long as the network requires it.

VII. RESOURCES AND SCHEDULE

The following tables show the funds budgeted, programmed or planned to procure, develop, implement, and maintain the hardware and software for COINS network security.

A. KSOS/TCP4

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	--	--	--
RDT&E	60	200	80	40	--	--	--
TOTAL	60	200	80	40	--	--	--

1000 of Dollars

The RDT&E Funds for 1980 are for the impact study. Funds for FY81-82 are for partitioning of the TAS functions and for integrating KSOS and TAS. The FY83 funding is to evaluate the cost benefits of using the KSOS/TCP4 combination in COINS.

B. Multi-Jurisdictional Security Protocols

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	--	--	--
RDT&E	--	--	--	100	50	--	--
TOTAL	--	--	--	100	50	--	--
1000 of Dollars							

The RDT&E funds for FY83-84 are to develop and install the software that collects the individual CASs, AAFs, and redistributes the sorted access authorizations to all access ring systems.

C. BLACKER

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	80	250	--	--	--	--
RDT&E	25	108	50	--	--	--	--
TOTAL	25	188	300	--	--	--	--
1000 of Dollars							

The RDT&E funds in FY80 through FY82 are to test the operation and user acceptance of BLACKER. The procurement funds are to acquire another BLACKER front-end for SOLIS and additional personal identification and authentication hardware.

D. BLACKER Application

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	--	--	--
RDT&E	--	25	50	75	--	--	--
TOTAL	--	25	50	75	--	--	--
1000 of Dollars							

The RDT&E funds over FY81-83 are for studies on how best to use or adapt BLACKER for COINS use.

E. Secure Network Front-End

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	?	?	--
RDT&E	--	--	--	180	350	300	130
TOTAL	--	--	--	180+	350+	300	130
1000 of Dollars							

The FY83 RDT&E funds are for the development of comprehensive specifications for a front-end suitable for use in the several networks expected to be available in the mid- to late 1980's. A portion of the FY83 funds is expected to be used to identify a suitable candidate hardware to implement the result.

During FY84, the RDT&E emphasis will be on studies and specifications for partitioning the front-end functions and integrating BLACKER and KSOS. The funds for FY85 and FY86 are for the development of a prototype for demonstration and evaluation. An undetermined amount of funds for procuring a suitable hardware base for the development will be required in FY84 and FY85.

F. Improved User Identification and Authentication

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	50	--	--	--	--	--	--
RDT&E	--	50	25	25	25	25	25
TOTAL	50	50	25	25	25	25	25
1000 of Dollars							

The procurement funds for FY80 are for a suitable badge reader. The RDT&E funds for FY81 are for interfacing it with BLACKER terminals. The balance of the RDT&E funds (FY82-86) are for evaluation and low-level tracking of new technology applicable to the problem.

G. Software Encryption

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	--	--	--
RDT&E	--	60	--	--	--	--	--
TOTAL	--	60	--	--	--	--	--
1000 of Dollars							

The RDT&E funds in FY81 are for the testing and additional development of the Crypt function in UNIX7 and the one-way encryption algorithm(s) for application to log-on protection.

H. File Output Labeling

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	--	--	--
RDT&E	--	50	80	50	--	--	--
TOTAL	--	50	80	50	--	--	--
1000 of Dollars							

The FY81 RDT&E funds are for the system study of where the file output labeling is most effectively done (for all of the various possibilities in COINS) and a design of how to do it. In FY82 and 83, the design will be implemented and tested.

I. Network Access Control to COINS

	FY80	FY81	FY82	FY83	FY84	FY85	FY85
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	300	--	--	--
RDT&E	--	--	150	300	100	--	--
TOTAL	--	--	150	600	100	--	--
1000 of Dollars							

The FY82 RDT&E funds are for a detailed design of a generalized gateway suitable for use with PLATFORM, IDHSC, AUTODIN II, etc. The FY83 and 84 RDT&E funds are for the implementation and test of the design. The procurement funds are for the acquisition of a suitable gateway machine.

J. NSO Support

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	50	50	50
Procurement	--	--	--	--	--	--	--
RDT&E	--	--	50	75	25	--	--
TOTAL	--	--	50	75	75	50	50
1000 of Dollars							

The RDT&E funds for FY82 through FY84 are to establish the detailed requirements for an NSO monitoring and surveillance

system. Implement and test the system. The O&M funds, FY84 through FY86, are for the development of additional NSO tools to assist in the security monitoring of the network and its use.

K. Security Architecture

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	--	--	--
Procurement	--	--	--	--	--	--	--
RDT&E	50	50	50	50	50	50	50
TOTAL	50	50	50	50	50	50	50
1000 of Dollars							

The RDT&E funds shown are to provide continued contractor support over the period shown.

SUMMARY OF COSTS

	FY80	FY81	FY82	FY83	FY84	FY85	FY86
O&M	--	--	--	--	50	50	50
Procurement	50	80	250	300	--	--	--
RDT&E	135	543	535	895	600	375	205
TOTAL	185	623	785	1195	650	425	255
X \$1000							

SCHEDULE

PROGRAM ELEMENT	FY80	FY81	FY82	FY83	FY84	FY85	FY86
KSOS/TCP4		▲					
Multi-Jurisdictional Security Control				▲			
BLACKER Test		▲					
BLACKER Applications			▲				
SNFE						▲	
Improved User ID & Authentication Techniques							▲
TAS/NAS Software Encryption		▲					
File/Output Labeling				▲			
Gateway Design (Network Access)						▲	
Network Security Officer Support						▲	
Architecture							▲

REFERENCES

1. TMA-3 - 1971, "Dissemination Controls for COINS", April 1, 1971, COINS PMO.
2. DCID 1/16 - Security of Foreign Intelligence in Automated Data Processing Systems and Networks, June 6, 1978.
3. Security Markings - DCID 1/7 - Control of Dissemination of Foreign Intelligence, May 11, 1976.
4. Security - DCID 1/14 - Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, May 13, 1976.
5. Privacy - Executive Order 12036.
6. COMSEC - WSCSB 4-11 - National Policy on Control of Compromising Emanations, June 1, 1976.
7. TAS Functional Specifications and User Command Language, J.P. Anderson Company, November 25, 1976.
8. Terminal Access System, User's Manual, Logicon, Inc., 1979.
9. Terminal Access System, Access Authorization File Maintenance (AAFM) User's Manual, Logicon, Inc., 1979.
10. "Password Security: A Case History", Morris, R., Thompson, K., Communications of the ACM, Vol 22, No. 11, November 1979, pp. 594-597.
11. COINS Network Security Issues, J.P. Anderson Company, July 31, 1976.
12. COINS-II Security Problems, Analysis and Implications, J.P. Anderson Company, March 7, 1978 (revised November, 1978).
13. Problems Associated with Accommodating Interactive Hosts in COINS-II (Interim Draft), ICA Corp., February 26, 1979.
14. Uniform Network Interactive Logon Sequence, Memorandum for the Record, R.A. Parke, January 19, 1978.
15. ADAPT I Final Functional and System Design Specification, Logicon, Inc., January 30, 1978.

16. "Gateway Techniques for Interconnection of Digital Networks", (draft) Report No. CSC-SD-77/4132, Computer Sciences Corporation, December 16, 1977.
17. "Techniques for Gateway PLATFORM with Other Digital Networks", (draft) Final Report, Contract MDA904-77-A00182, System Control Inc., December, 1977.
18. COINS-II: Which Way to Mecca?, J.P. Anderson Company, November 21, 1978.
19. USIB 9.1/20 - Physical Security Standards for Sensitive Compartmented Information.
20. "Management of the COINS Experiment"
21. "Recommendations of the ASD(I)'s Review Group", February, 1973.

STAT

Approved For Release 2003/08/18 : CIA-RDP83T00573R000100140001-8

Approved For Release 2003/08/18 : CIA-RDP83T00573R000100140001-8